SNI

Standar Nasional Indonesia

SNI 19-7125-2005

Teknologi informasi – Teknik keamanan – Panduan teknik untuk penggunaan dan manajemen jasa Pihak Ketiga Terpecaya

ICS 35.040

Badan Standardisasi Nasional

BSN
Gd. Manggala Wanabakti
Blok IV, Lt. 3,4,7,10.
Telp. +6221-5747043
Fax. +6221-5747045
Email: dokinfo@bsn.go.id
www.bsn.go.id

Diterbitkan di Jakarta

Prakata

Standar Nasional Indonesia (SNI) *Teknologi informasi – Teknik keamanan – Panduan teknik untuk penggunaan dan manajemen jasa Pihak Ketiga Terpercaya* ini mengadopsi secara identik ISO/IEC TR 14516:2002, *Information technology – Security techniques – Guidelines for use management of Trusted Third Party services* dengan metode lembar sampul (*cover sheet*).

SNI ini disusun oleh Panitia Teknis 35-01, Panitia Teknis *Transaksi Informasi melalui Media Elektronik*.

Panitia Teknis 35-01 memutuskan untuk melakukan adopsi identik ISO/IEC TR 14516 atas dasar beberapa pertimbangan berikut:

- Keterbatasan pengetahuan
- Waktu yang lebih cepat
- Efisiensi biaya
- Akseptabilitas secara internasional
- Belum tersedianya UU yang terkait dengan penyediaan Sistem Keamanan Transaksi Informasi melalui Media elektronik, membutuhkan adanya standar sebagai pedoman industri
- Citra positif bagi industri dengan mengadopsi standar internasional

Dalam standar ini daftar standar tentang *Teknologi informasi – Teknik keamanan – Panduan teknik untuk penggunaan dan manajemen jasa Pihak Ketiga Terpercaya* yang identik dengan standar international dalam ISO/IEC TR 14516:2002 termasuk amandemennya, diberikan dalam acuan normatif.

CONTENTS

Table of Figures

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, the joint technical committee may propose the publication of a Technical Report of one of the following types:

— type 1, when the required support cannot be obtained for the publication of an International Standard, despite repeated efforts;

— type 2, when the subject is still under technical development or where for any other reason there is the future but not immediate possibility of an agreement on an International Standard;

— type 3, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example).

Technical Reports of types 1 and 2 are subject to review within three years of publication, to decide whether they can be transformed into International Standards. Technical Reports of type 3 do not necessarily have to be reviewed until the data they provide are considered to be no longer valid or useful.

Attention is drawn to the possibility that some of the elements of this Technical Report may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 14516, which is a Technical Report of type 3, was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.842.

Introduction

Achievement of adequate levels of business confidence in the operation of IT systems is underpinned by the provision of practical and appropriate legal and technical controls. Business must have confidence that IT systems will offer positive advantages and that such systems can be relied upon to sustain business obligations and create business opportunities.

An exchange of information between two entities implies an element of trust, e.g. with the recipient assuming that the identity of the sender is in fact the sender, and in turn, the sender assuming that the identity of the recipient is in fact the recipient for whom the information is intended. This "implied element of trust" may not be enough and may require the use of a Trusted Third Party (TTP) to facilitate the trusted exchange of information.

The role of TTPs includes providing assurance that business and other trustworthy (e.g. governmental activities) messages and transactions are being transferred to the intended recipient, at the correct location, that messages are received in a timely and accurate manner, and that for any business dispute that may arise, there exist appropriate methods for the creation and delivery of the required evidence for proof of what happened. Services provided by TTPs may include those necessary for key management, certificate management, identification and authentication support, privilege attribute service, non-repudiation, time stamping services, electronic public notary services, and directory services. TTPs may provide some or all of these services.

A TTP has to be designed, implemented and operated to provide assurance in the security services it provides, and to satisfy applicable legal and regulatory requirements. The types and levels of protection adopted or required will vary according to the type of service provided and the context within which the business application is operating.

The objectives of this Recommendation | Technical Report are to provide:

a) Guidelines to TTP managers, developers and operations' personnel and to assist them in the use and management of TTPs; and

b) Guidance to entities regarding the services performed by TTPs, and the respective roles and responsibilities of TTPs and entities using their services.

Additional aspects covered by this Recommendation | Technical Report are to provide:

a) An overview of the description of services provided;

b) An understanding of the role of TTPs and their functional features;

c) To provide a basis for the mutual recognition of services provided by different TTPs; and

d) Guidance of interworking between entities and TTPs.

TECHNICAL REPORT

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – GUIDELINES FOR THE USE AND MANAGEMENT OF TRUSTED THIRD PARTY SERVICES

1 Scope

Associated with the provision and operation of a Trusted Third Party (TTP) are a number of security-related issues for which general guidance is necessary to assist business entities, developers and providers of systems and services, etc. This includes guidance on issues regarding the roles, positions and relationships of TTPs and the entities using TTP services, the generic security requirements, who should provide what type of security, what the possible security solutions are, and the operational use and management of TTP service security.

This Recommendation | Technical Report provides guidance for the use and management of TTPs, a clear definition of the basic duties and services provided, their description and their purpose, and the roles and liabilities of TTPs and entities using their services. It is intended primarily for system managers, developers, TTP operators and enterprise users to select those TTP services needed for particular requirements, their subsequent management, use and operational deployment, and the establishment of a Security Policy within a TTP. It is not intended to be used as a basis for a formal assessment of a TTP or a comparison of TTPs.

This Recommendation | Technical Report identifies different major categories of TTP services including: time stamping, non-repudiation, key management, certificate management, and electronic notary public. Each of these major categories consists of several services which logically belong together.

2 References

2.1 Identical Recommendations | International Standards

– IT U-T Recommendation X.509 (2001) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.*

– ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*

– ITU-T Recommendation X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework.*

2.2 Paired Recommendations | International Standards equivalent in technical content

– CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

2.3 Additional References

– ISO/IEC 9798-1:1997, *Information technology – Security techniques – Entity authentication – Part 1: General.*

– ISO/IEC 11770-1:1996, *Information technology – Security techniques – Key management – Part 1: Framework.*

– ISO/IEC 11770-2:1996, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques.*

– ISO/IEC 11770-3:1999, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques.*

– ISO/IEC TR 13335-1:1996, *Information technology – Guidelines for the management of IT Security – Part 1: Concepts and models for IT Security.*

- ISO/IEC TR 13335-2:1997, *Information technology – Guidelines for the management of IT Security – Part 2: Managing and planning IT Security.*
- ISO/IEC TR 13335-3:1998, *Information technology – Guidelines for the management of IT Security – Part 3: Techniques for the management of IT Security.*
- ISO/IEC TR 13335-4:2000, *Information technology – Guidelines for the management of IT Security – Part 4: Selection of safeguards.*
- ISO/IEC 13888-1:1997, *Information technology – Security techniques – Non-repudiation – Part 1: General.*
- ISO/IEC 13888-2:1998, *Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques.*
- ISO/IEC 13888-3:1997, *Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques.*
- ISO/IEC WD 15443, *Information technology – Security techniques – A framework for IT security assurance.*

3 Definitions

NOTE – Throughout this Recommendation | Technical Report the term entity may refer to a human being, an organisation, a hardware component or a piece of software.

For the purpose of this Recommendation | Technical Report the definitions given in CCITT Rec. X.800 and ISO 7498-2 apply: access control, accountability, audit, audit trail log, availability, confidentiality, data integrity, decipherment, digital signature, encipherment, entity authentication, integrity, key, key management, notarisation, non-repudiation, security audit, security audit trail and signature.

For the purpose of this Recommendation | Technical Report the definitions given in ISO 8402 apply: audit/ assessment.

For the purpose of this Recommendation | Technical Report the definitions given in ITU-T Rec. X.509 | ISO/IEC 9594-8 apply: attribute certificate, certificate and certification authority (CA).

For the purpose of this Recommendation | Technical Report the definition given in ISO/IEC 9798-1 applies: token.

For the purpose of this Recommendation | Technical Report the definition given in ISO/IEC 9798-5 applies: accreditation authority.

For the purpose of this Recommendation | Technical Report the definitions given in ITU-T Rec. X.810 | ISO/IEC 10181-1 apply: private key, public key, seal, secret key and trusted third party.

For the purpose of this Recommendation | Technical Report the definitions given in ITU-T Rec. X.811 | ISO/IEC 10181-2 apply: authentication certificate and authentication information (AI).

For the purpose of this Recommendation | Technical Report the definitions given in ITU-T Rec. X.813 | ISO/IEC 10181-4 apply: evidence generator and notary.

For the purpose of this Recommendation | Technical Report the definitions given in ISO/IEC 11770-1 apply: asymmetric cryptographic technique, symmetric cryptographic technique and time stamp.

For the purpose of this Recommendation | Technical Report the definitions given in ISO/IEC TR 13335-1 apply: asset, authenticity, impact, IT security, IT security policy, reliability, residual risk, risk, risk analysis, risk management, safeguard, system integrity, threat and vulnerability.

For the purpose of this Recommendation | Technical Report the definitions given in ISO/IEC 13888-1 apply: non-repudiation of approval, non-repudiation of creation, non-repudiation of delivery, non-repudiation of knowledge, non-repudiation of origin, non-repudiation of receipt, non-repudiation of sending, non-repudiation of submission, and non-repudiation of transport.

For the purpose of this Recommendation | Technical Report the following additional definitions apply:

3.1 attribute Authority (AA): An entity trusted by one or more entities to create and sign attribute certificates. Note that a CA may also be an AA.

3.2 registration Authority (RA): An entity who is responsible for identification and authentication of subjects of certificates, but is not a CA or an AA, and hence does not sign or issue certificates. An RA may assist in the certificate application process, revocation process, or both.

4 General Aspects

A Trusted Third Party (TTP) is an organisation or its agent that provides one or more security services, and is trusted by other entities with respect to activities related to these security services.

A TTP is used to offer value-added services to entities wishing to enhance the trust and business confidence in the services that they receive and to facilitate secure communications between business trading partners. TTPs need to offer value with regard to confidentiality, integrity and availability of the services and information involved in the communications between business applications. TTPs should be able to interoperate with each other and with the entities.

Entities should be able to choose which TTP they will use to provide the required services. Also, TTPs should be able to choose the entities to which they will provide services.

To be effective, TTPs generally should:

a) operate within a legal framework which is consistent among the participating entities;

b) offer a range of services, with minimum services clearly defined;

c) have defined policies, in particular a public security policy;

d) be managed and operated in a secure and reliable manner, based on an information security management system and trustworthy IT systems;

e) conform to national and international standards, where applicable;

f) follow an accepted best code of practice;

g) publish practice statements;

h) record and archive all evidence relevant to their services;

i) allow for independent arbitration, without compromising security;

j) be independent and impartial in their operation, (e.g. accreditation rules); and

k) assume responsibility of liability within defined limits for availability and quality of service.

4.1 Basis of Security Assurance and Trust

The use of a TTP and its services depends on the fundamental observation that the services provided by the TTP will be trusted by other TTPs and entities. This trust results from the confidence that the TTP is managed correctly and its services are operated securely. Therefore it should give assurance that the TTP itself and the services it provides are according to the defined policies. Especially, the security policy should cover all security aspects related to the management of the TTP and the operation of the services.

The confidence can be established through evidence of the management and operational TTP aspects. Evidence should be given that the management aspects are proper and sufficient to completely achieve the objectives, that the management system is effective, suitable to minimise risks and to counter threats, and the safeguards are documented and understood by personnel, not outdated or superseded and are implemented properly.

To gain confidence in the management and operational aspects a TTP especially should provide evidence that:

a) there is an appropriate Security Policy in place;

b) security problems have been addressed by a combination of correctly implemented security procedures and mechanisms;

c) the operations are being carried out correctly and in keeping with a clearly defined set of roles and responsibilities;

d) the interfaces and procedures for communicating with entities are appropriate for the functions to be performed and are correctly used;

e) rules and regulations are followed by management and staff, and are consistent with a stated or targeted level of trustworthiness;

f) the quality of the processes, operations and working practices have been suitably accredited;

g) the TTP meets its contractual obligations according to a formal contract with its users;

h) there is a clear understanding and acceptance of the liability aspects;

i) compliance with laws and regulations is maintained and audited;

j) known threats and safeguards to mitigate those threats are clearly identified;

k) a Threat and Risk Assessment is done initially and reviewed/updated on a regular basis to ensure that confidentiality, integrity, availability and reliability requirements are met;

l) proper organisational and personnel measures are met;

m) the trustworthiness of the TTP can be relied upon and that it can be checked and verified, and

n) that the TTP is monitored by some type of administrative authority to oversee that its operation is within its accreditation rules.

Details are discussed in clause 5, Management and Operational Aspects of a TTP.

Different types of business and different applications will require different levels of trust and may require different levels of strength for the applied protection mechanisms and procedures. For example, the level of trust required for the authentication of administrative transactions may be different from that required for financial transactions, which may be different from that required in some military applications. Different levels of trust result from different security policies and standards and how well they are correctly implemented.

4.2 Interaction between a TTP and Entities Using its Services

From a communication point of view the location of the TTP and entities can be arranged in different configurations: in-line, on-line and off-line. An example of each configuration is given in 4.2.1 through 4.2.3.

Some TTP services may be based on different configurations, therefore the configuration that is adopted will influence the services the TTP will be capable of fulfilling, e.g. timeliness of the exchange, denial of service, recording of proof, and their characteristics, such as delay of revocation of a certificate.

4.2.1 In-line TTP Services

An in-line TTP is needed when two or more entities belong to different security domains and do not use the same security mechanisms. In this case the entities are unable to operate direct, secure exchanges. However, a TTP positioned directly in the communication path between the entities can facilitate secure exchanges between these entities as illustrated in Figure 1.

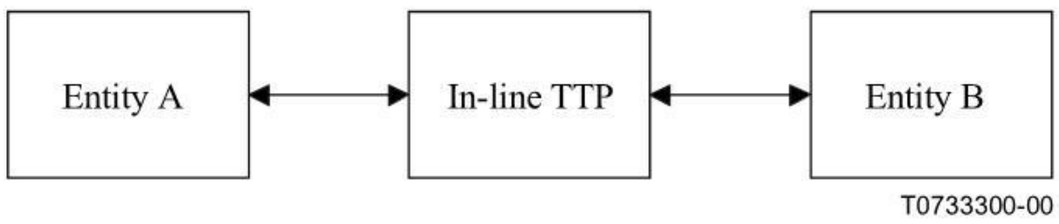

Figure 1 – In-line TTP Service Between Entities

In-line TTP services may include authentication, translation and privilege attribute services, and the TTP may play a role in providing non-repudiation, access control, key recovery, confidentiality and integrity services of transmitted data.

4.2.2 On-line TTP Services

When one or both entities request an on-line TTP to provide or register security-related information, the TTP is involved in all first time secure exchanges between the entities. However, the TTP is not required for follow-up exchanges and is not positioned in the communication path between the entities as illustrated in Figure 2.

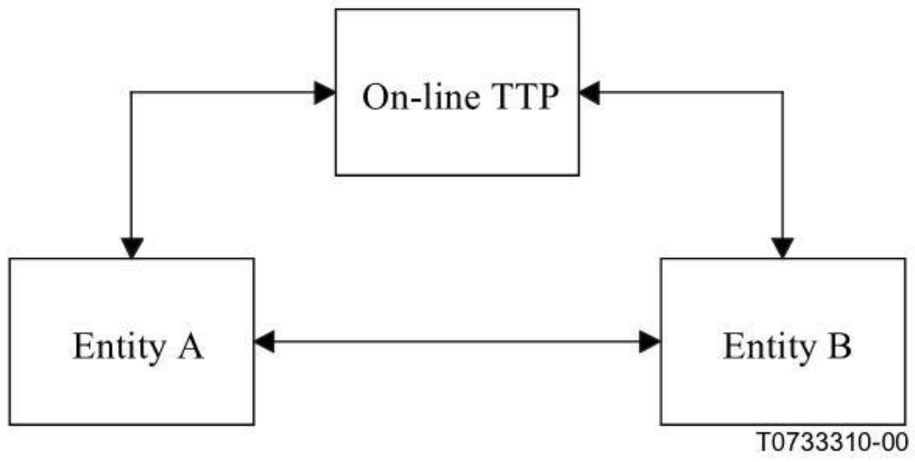

Figure 2 – On-line TTP Service Between Entities

On-line TTP services may include authentication, certification and privilege attribute services, and the TTP may play a role in providing non-repudiation, access control, key management, delivery of messages, time stamping, confidentiality and integrity services.

4.2.3 Off-line TTP Services

A third type of configuration for the provision of TTP services is Off-line. The TTP does not interact directly with the entities during the process of secure exchanges between the entities. Instead data generated previously by the TTP is used by the entities as illustrated in Figure 3 with the dotted lines.

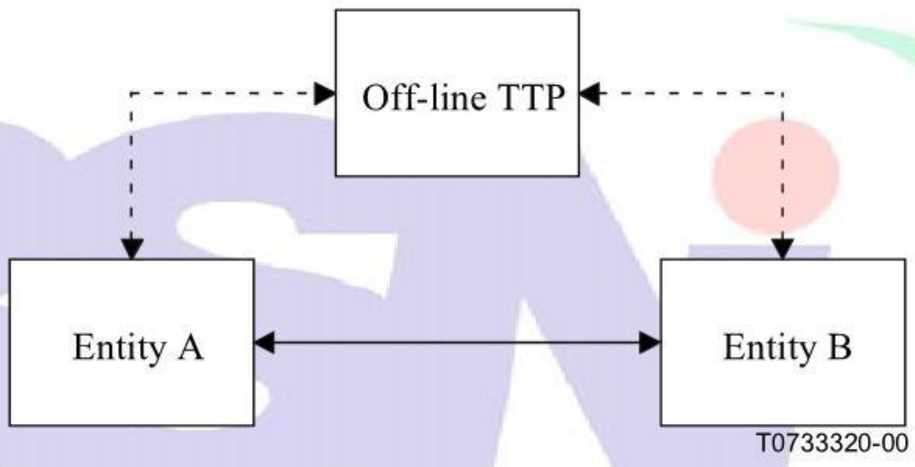

Figure 3 – Off-line TTP Service Between Entities

Off-line TTP services may include authentication, certification, privilege attribute, non-repudiation, key distribution and key recovery services.

4.3 Interworking of TTP Services

A TTP can offer several services, which are described in clause 7. All services may be provided by a single TTP or they may be provided by more than one TTP. The services can also be provided from one or more locations. In the latter case the tasks and duties should be defined and stated in a formal contract, and the technical and organisational impacts should be taken into account. Depending on the TTP architecture (responsibility and location) there may be additional requirements, especially security related ones, that should be considered by the TTP management.

NOTE – Each service may have specific security requirements that should be fulfilled. Where possible, it is generally recommended to split the management and operational aspects of a TTP into general and specific aspects related to each service. A modular structured management system is much more easily handled if changes occur, especially the identification of security critical impacts when changes are made.

5 Management and Operational Aspects of a TTP

For the management and operation of a TTP there should exist an umbrella strategy which takes into account the issues in the following subclauses. The commitment of a TTP to provide security related services should take the form of a formal documented policy. It is recommended that a TTP should use guidelines for the protection of its services. General guidelines for the management of IT security (GMITS) can be found in ISO/IEC TR 13335-1, 13335-2, 13335-3 and 13335-4 in Annexes A-H of 13335-4.

Depending on the services provided by a TTP there are a lot of decisions that have to be made. There is a need not only to define policies for the services, but also to define more specific policies, such as signature creation and validation policies. Both will lead to technical implications and consequences that should be considered in advance. Additionally there are dependencies between technical and non-technical equipment, e.g. the provision of directory services via the Online Certificate Status Protocol or the Certificate Revocation List. All those factors will lead to technical implementations and consequences that should be reflected in advance. An example of a security policy which deals with public key certificates can be found in RFC 2527, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

5.1 Legal Issues

In addition to the basic accuracy of the particular services provided, e.g. accurate time for a time stamping authority, a TTP will inherit broad-ranging responsibilities from the expectations of its users. These responsibilities will include flawless provisions for confidentiality, integrity, availability, access control, accountability, authenticity, reliability, privacy, ethical (such as legitimate use), legal (i.e. laws and regulations), techniques and mechanisms, and financial aspects. Accidental or deliberate breaches of these responsibilities by a TTP may lead to substantial loses by its users, who will attempt to recover these losses from the TTP. In order to manage the expectations of its users and limit its liability, a clearly defined, legally binding contract between the TTP and its users should be established. As a minimum this contract should address the legal issues for the following topics:

a) liability;

b) privacy, especially with the respect to data protection law;

c) copyright and intellectual property;

d) use of cryptography;

e) lawful interception and lawful access;

f) legality of a binding service such as digital signatures;

g) anonymity of entities;

h) right to investigate, e.g. credentials;

i) legislative and regulatory requirements applicable to the jurisdiction and industry;

j) the types of service to be provided;

k) access arrangements including permitted methods of access, procedures by which users can be authorised (and authorised users changed);

l) procedures for problem resolution (including authorised points of contact);

m) responsibilities concerning hardware and software requirements, management and change control; and

n) arrangements for reporting, notification, and investigation of security incidents.

The TTP's commitments and liability should be consistent with its financial capacity and warrants or pledges it received from other entities. Entities should have a commitment that the information they provide to a TTP is protected from disclosure, unless otherwise specified within their contract. Legal demands for protecting personal information have to be met by a TTP, especially those relating to the appropriate technical and organisational protection of databases containing personal data.

Electronic commerce is international by nature and TTPs should comply with all legal obligations with respect to national and international laws, regulations and treaties. Compliance with some of these obligations may have a significant impact on the design or the implementation of a TTP.

The concepts of liability, and the basic legal framework may differ from nation to nation. Therefore, general guidance will need to be adapted to meet the needs of individual legal systems. In cases where national legislation regarding TTPs is not consistent across national boundaries, TTPs who wish to allow their users to communicate across these boundaries, should have a special contractual agreement in place to address cross-jurisdictional differences.

When TTPs are interworking across national boundaries they have to be aware of the legal consequences in such an environment with regard to the potential differences or incompatibilities between their security policies and practice statements.

5.2 Contractual Obligations

Formal contracts between a TTP and entities using its services should clearly state the responsibilities of the TTP, the quality of the service to be provided, as well as the responsibilities of the entities using TTP services.

The contract should explain the managerial and organisational policy of the TTP, as well as the operational procedures. The TTP should also issue a Practice Statement that describes what entities may expect from the TTP services in order to clearly define publicly the operational aspects and requirements, quality of service, ethical issues, and subscriber's fees.

The contract should specify provisions clearly describing how the TTP complies with relevant legislation and regulations. The contract should specify the jurisdiction of operation and the jurisdiction under which disputes will be resolved.

Accidental or deliberate errors by a TTP may lead to substantial damage to business. In order to have sufficient confidence to use TTP services, the contract should define the limits of the TTP's liability with its users. Where applicable, the liability should be covered by an appropriate insurance contract in case of a dispute. The required coverage should be defined in the contract between the TTP and its users.

The contract should include a list of all matters concerning liabilities between the TTP and its users so that the users can access adequate professional advice in order to obtain appropriate legal assistance on any matter arising from the provision and use of the TTP's services.

The contract should describe the intended uses of the service and its service parameters, and should enable the service to be withdrawn if either contracting party is using it improperly or illegally.

The contract could have provisions that clearly state that an independent and impartial party (arbitrator) may be requested to assist in dispute resolution between the TTP and its users.

The contract should specify how the privacy of personal and other sensitive information will be protected, and the circumstances under which disclosure may occur.

5.3 Responsibilities

A TTP should define the extent to which responsibility is taken for the secure operation of its service. In addition, the TTP should delineate the extent of the liabilities that may be accepted in respect of security breaches.

The responsibilities of the TTP, as well as those of the user, should be clearly stated in any formal contract that is set up between the user and the TTP. Most responsibilities should be part of a contract, and some should at least be defined as a matter of business, while others should be standard qualities of service.

Other documents, such as those containing the definition of the services to be provided, the service agreement and any technical annexes included as attachments to the contract, also determine respective responsibilities of the various entities involved. These documents form part of the overall contractual agreement.

5.4 Security Policy

A TTP undertakes certain obligations in offering and operating security related services, based on confidence and trust in the services being offered, and a formal documented security policy for the organisation offering the service.

A TTP's security policy is a vital instrument to describe all essential and important activities in order to establish trust, and to gain confidence in the management of the TTP and the operation of its services. Therefore, a TTP security policy should not only cover specific security issues but also contain all TTP service related aspects. The development and maintenance of a TTP's security policy should be done in a systematic and logical manner.

As discussed in ISO/IEC TR 13335-3, Annex A, a TTP's security policy should consist of two parts:

a) a general security policy which expresses concisely the non-technical aspects regarding security and confidence in the TTP services; and

b) a technical security policy which expresses concisely all technical aspects regarding security related functionality and trust together with descriptions of routines, procedures, etc. related to technical aspects.

A rigorous security related evaluation of current TTP services verifies the confidence in the technical systems according to the measure of confidence in the TTP's security policy.

A TTP's security policy is of vital importance in maintenance of confidence between systems, in specifying the basis for continuous (internal) review and periodical (internal and external) audit of security, and confidence to the systems and the organisation which operates the service.

The commitment of a TTP to provide a security related service should take the form of a formal and documented security policy. The security policy should identify all relevant targets, objects and potential threats related to the services provided and the safeguards required to avoid or limit the effects of those threats. It should describe the rules, directives and procedures regarding how the specified services and the associated security assurance are granted.

5.4.1 Security Policy Elements

The content of a TTP's security policy will depend upon the services provided by the TTP. The security policy should be a framework that addresses the security issues related to various elements. The technical elements of the TTP's security policy form the basis for a technical security related assessment. As discussed in ISO/IEC TR 13335-2, the security policy of a TTP should include at least the following elements:

a) IT security requirements, e.g. in terms of confidentiality, integrity, availability, authenticity, accountability and reliability, particularly with regard to the view of the information owners;

b) organisational infrastructure and assignment of responsibilities;

c) integration of security into system development and procurement;

d) awareness and training;

e) directives and procedures;

f) definition of classes for information classification;

g) risk management strategies;

h) contingency planning;

i) personnel issues, with special attention to personnel in positions requiring trust such as maintenance personnel and system administrators;

j) legal and regulatory obligations;

k) outsourcing management; and

l) incident handling.

The implementation of a TTP's security policy covering technical, administrative and organisational requirements for security should have special emphasis on the following requirements:

a) assurance that the TTP performs its functions in such a way that system integrity cannot be impaired or harmed;

b) the integrity of entity data, that it is complete, unmodified and that its source and origin can be verified;

c) that authorised entities are ensured the availability of and access to the services and information they are entitled to;

d) the confidentiality of sensitive and private information entrusted by the entity to the TTP; and

e) procedures to audit the TTP's system security.

5.4.2 Standards

TTPs should use standards when relevant and applicable. Standards may include international, national, regional, industry sector, and corporate standards or rules, selected and applied according to the security requirements of their organisations. The benefits include interoperability, integrated security, consistency, portability and interworking between organisations. If different organisations develop and use their own systems or products based on proprietary standards, there is the potential for short-term problems of interoperability with the various approaches. Standards need to be examined at two levels; detailed standards for specific technologies and their use, and standards for interoperability between the different technologies.

5.4.3 Directives and Procedures

Directives and procedures are required elements of a TTP security policy. They include the required rules and regulations set up by the organisation, and the guidance procedures that are necessary for the organisation to provide services to its users.

5.4.4 Risk Management

In order to gain an acceptable level of IT system security a TTP should implement methods for risk management. The risk management process for security of a TTP's IT system should be based on a detailed risk analysis or a combined approach. An assessment of all information should be done to determine the sensitivity of the information and the appropriate levels of protection to maintain its confidentiality, integrity and availability. Threats, risks and safeguards should be reassessed periodically. The guidance for choosing an appropriate strategy of risk analysis and a detailed description of the risk analysis process can be found in ISO/IEC TR 13335-3. Based on the results of risk analysis appropriate safeguards should be chosen, tested and implemented.

5.4.5 Selection of Safeguards

The TTP is subject to many accidental or deliberate threats that may be of a natural or human origin. The TTP should be protected against such threats with safeguards designed to reduce vulnerabilities by mitigating the impact of unwanted incidents and/or by enhancing facilitation of recovery.

Security measures, practices and procedures should take into account all relevant technical, organisational, clerical, commercial, human and legal aspects, and be integrated into or coordinated with the normal measures, practices and procedures of the organisation.

Security levels, costs, measures, practices and procedures should be appropriate and proportional to the severity of threats, potential impacts of risks and the level of assurance granted.

Detailed guidance for the selection of safeguards can be found in ISO/IEC TR 13335-4, clauses 8 to 11.

5.4.5.1 Physical and Environmental Measures

Physical and environmental security controls should be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organisation's physical and environmental security program should address the physical access control, fire protection, supporting utilities (electrical, plumbing and air-conditioning), protection against theft, cabling, etc.

Periodically, an organisation should practice business continuity planning which addresses these aspects in order to keep its critical business functions operating in the event of disruptions, both large and small, or in the event of a disaster. Business continuity planning should include incident handling capabilities that provide the ability to react quickly and efficiently to disruptions in normal processing (see also 5.4.7.3, Contingency Planning).

5.4.5.2 Organisational and Personnel Measures

An organisation should have security policies which contain rules, directives and practices describing how assets are managed, protected and distributed within the organisation. All critical functions which support the business processes should be identified and documented, with personnel assigned and accountable for those functions.

An organisation should have the commitment from all levels of management to support the requirements of IT security. There should be a willingness to address IT security requirements and to allocate the resources to fulfil those requirements.

An organisation should have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Appropriate assignment and demarcation of responsibilities should ensure that all-important tasks are accomplished and that they are performed in an efficient way.

An organisation should ensure effective administration of an entity's computer access to maintain system security, including user account management, auditing and timely modification or removal of access.

5.4.5.3 IT Specific Measures

A TTP that provides security related services relies heavily on IT systems. Therefore specific IT safeguards are needed to make them secure and proper. These specific safeguards can be divided into technical, communications and networking categories. Safeguards may be selected according to a detailed assessment, to security concerns and threats, or the type of IT system.

a) Measures according to security concerns and threats consist of safeguards for confidentiality, integrity, availability and accountability:

   ∞ Confidentiality – The security of a TTP service may rely on a widely (system wide) used key, e.g. certification keys. The protection of those keys could be realised physically by use of trustworthy hardware and logically by shared secret schemes.

   ∞ Integrity – Sensitive information exchanged on the User-TTP interface, for on-line, off-line and out-of-band communication modes, should be protected from alteration, interruption and blocking.

   ∞ Availability – TTPs should implement mechanisms which guarantee their users access to TTP services when required. The special occurrence of non-availability, i.e. denial of service, could have a great impact on TTP activity. Appropriate mechanisms preventing telecommunications "flooding", routing problems and disruption of service should be taken into consideration.

- ∞ Accountability – The responsibilities and accountability of all activities must be defined for TTPs and the users of TTP services. TTPs should implement proper mechanisms so that every event and action can be traced to the responsible entity. The accountability can be accomplished through the use of monitoring of security audit trails, and by auditing on a regular basis. Adequate audit logs should be maintained to provide an audit trail of all actions, transactions, processes, etc. The ownership of sensitive information and the associated security responsibilities along with auditing, are important to provide effective TTP services.

b) Measures according to the type of IT system consist of safeguards for access control:

- ∞ Access Controls – The protection against the unauthorised use of TTP services can be provided by access control safeguards. The implementation of appropriate mechanisms should be considered in the following areas:
  - identification and authentication;
  - physical access control;
  - logical access control;
  - cryptography; and
  - privilege management.

Details on access control can be found in ISO/IEC TR 13335-4 and ITU-T Rec. X.812 | ISO/IEC 10181-3.

5.4.6 Implementation Aspects of IT Security

5.4.6.1 Awareness and Training

Effective computer security awareness, training and education should be required by all personnel within the TTP organisation to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems. Without the acceptance and involvement of personnel at all levels, a security awareness programme cannot succeed. It is especially critical for management to be aware of the need for security and to promote the awareness of security for their staff. The aim of an awareness programme is to convince personnel that significant risks to IT systems do exist and that information loss, or unauthorised modification or disclosure, could have major consequences for the organisation and its personnel. Details on awareness and training can be found in ISO/IEC TR 13335-2.

5.4.6.2 Trustworthiness and Assurance

The security assurance granted by TTPs should result from the:

a) selection of appropriate mechanisms, with regard to the services provided and the Security Policy;

b) proper implementation of these mechanisms, particularly with regard to physical security aspects, environment, business continuity, etc.; and

c) operation of these mechanisms, depending on the definition and respect of appropriate procedures, particularly with regard to personnel management, information classification, authorisation, incident handling, etc.

TTPs should utilise only trustworthy systems in performing their services. A formal evaluation of systems could prove their trustworthiness. Details for evaluation criteria to assist in deciding what minimum level of assurance should be in place for TTPs can be found in ISO/IEC 15408 (Common Criteria).

For a TTP to be trustworthy, it must be operated in accordance with its specifications. Certification is the procedure by which an independent party gives assurance that a product, process or service conforms to specified requirements. The certification process consists mainly of a document review and a technical evaluation by an impartial certification body.

Such a conformity certification of a TTP will give assurance that the security claimed by a TTP is in fact provided. Entities using TTP services therefore can use such security TTP conformance certifications as a basis for determining the level of trust they can place on a TTP.

Depending on the TTP services to be supported, the conformity certification process should include an analysis of:

a) conformance to relevant national and international laws and regulations governing their status, activities and performance;

b) conformance to technical standards;

c) conformance of the Security Policy;

d) conformance to sectorial or professional specific rules; that they are well defined, implemented and carried out both in the administrative and in the technical sense;

e) conformance to best codes of practice; and

f) the adequacy of the security measures with respect to the threats, risks, and Security Policy.

The decision by management of an organisation to obtain a TTP conformity certification may have significant impacts on the design and implementation of the TTP. An example of security requirements for TTPs can be found in the German Digital Signature Act and in accompanying regulations. Certification Authorities that issue certificates to TTPs must also obtain a conformity certification. An example of requirements for conformity certification of Certification Authorities can be found in B.2.

5.4.6.3 Accreditation of TTP Certification Bodies

The level of trust that users can place in a TTP can be increased if the TTP certification body is accredited under a scheme of relevance to the application. Accreditation ensures that the procedures of different TTP certification bodies are similar and the results of certification by different certification bodies are comparable. Accreditation is defined in ISO/IEC Guide 2. Accreditation of a TTP certification body means that the TTP certification body is widely recognised as competent and reliable in the provision of TTP certification services. Therefore accreditation of TTP certification bodies is an additional means of providing TTP service quality assurance because accrediting organisations are independent and operate according to widely accepted rules.

The accreditor assesses the procedural and technical aspects of TTP certification bodies management system according to ISO/IEC Guide 61 or other similar schemes such as the European 450xx series of standards.

Accreditation of a TTP certification body is a means of ensuring the quality of the work of the TTP certification body, but says nothing about the services provided by a particular TTP. The TTP defines the services they provide and the TTP certification body certifies how well they are conducted.

5.4.7 Operational Aspects of IT Security

5.4.7.1 Audit/Assessment

While evaluation is a means to prove the trustworthiness of IT systems, audit and assessment are the means to gain confidence and trust in the documented security policy and the realised security management system offering the TTP services. Evaluation is used in the context of IT system security inspections and the means to examine against evaluation criteria (details can be found in ISO/IEC 15408). Audit is used in the context of management reviews or baseline checks and the means to examine that the elements are known, documented and realised. Assessment is used in the context of product/process improvement and means to examine its strengths and weaknesses. All examinations are conducted periodically or upon request.

The aim of a security audit is to determine whether security policies are implemented effectively and achieve the desired objectives. A security audit is based on a review of the existing documents and an inspection of the implemented mechanisms and security controls, therefore, a TTP should have up-to-date, proper and adequate documentation.

Entities using TTP services may require that inspections and audits be carried out in order to check and validate the level of security actually granted by the TTP. They may request that audits be carried out by their own internal audit teams, or by external independent auditors. Audits can also be initiated by the TTP with the objective of reviewing its own security, its own risks or in providing evidence of its good practice to entities. Accreditation bodies may also require that audits be conducted. Audits can be initiated as a result of a number of different circumstances including: periodically (e.g. annually), upon request, after a major change or after an incident. Audits may consider the operational aspects of a TTP such as:

a) Security Policy;

b) selection of security mechanisms;

c) implementation of security mechanisms;

d) organisation;

e) procedures;

f) change management;

g) personnel (skills, training, etc.);

h) physical security;

i) financial aspects;

j) liability insurance, where applicable; and

k) documentation.

Audits should be carried out according to the usual applicable professional rules and practices. In particular, auditors, whether internal or external, should respect strict confidentiality rules. Accreditation bodies should impose directives on how to conduct audits. When audit reports are released to the general public or entities using the TTP services, the reports should be checked carefully to ensure that they do not contain any information that may be used to weaken the TTP's security.

NOTE – A description and details on quality audit and assessment procedures can be found in ISO 8402.

5.4.7.2 Incident Handling

A TTP should act in a timely and coordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents should be reported as soon as possible after the incident is detected. There should be procedures to cope with specific security events detected by, or brought to the knowledge of the TTP, e.g. the compromise of a secret key or a public/private key pair, or the loss of a personal security token. These procedures should be part of the TTP's Incident Analysis Scheme (IAS).

Breaches of security by entities, whether accidental or intentional should be difficult, and where possible, any attempted abuse of access rights by an entity should be detectable by the TTP.

5.4.7.3 Contingency Planning

The continuity of TTP services should be protected from the effects of failures or disasters. There should be a managed process in place for developing and maintaining procedures for contingencies. The contingency planning should cover the following:

a) identifying critical business functions;

b) identifying internal and external resources that support critical functions and services;

c) choosing a strategy for continuity;

d) establishing plans and procedures;

e) implementing plans and procedures; and

f) testing and updating plans and procedures.

Detailed guidance on contingency planning can be found in ISO/IEC TR 13335-3 and several national standards documents.

5.5 Quality of Service

General requirements for the quality of service are: reliability, availability, user friendliness, efficiency, correct implementation, documentation and access control.

5.6 Ethics

TTP services should be provided and used in such a manner that the rights and legitimate interests of all entities involved are respected.

5.7 Fees

TTPs may charge subscriber's fees for the use of their services. A schedule of all relevant fees should be made available if requested by the entities using these services, and the entities should be notified under which circumstances fees may change.

6 Interworking

Interworking requires a number of TTPs and entities to be connected together as a network with clearly defined interfaces, protocols and data formats to enable interworking to take place. Each TTP provides services to entities within its own domain according to its own security policy. There are several means of interaction including: TTP-Users; User-User; TTP-TTP; and where applicable, TTP-Law Enforcement Agency.

A TTP could have trust agreements with other TTPs to form a network, thus allowing an entity of one TTP to communicate securely with the entities of other TTPs. Where one TTP cannot provide all of the required services, the trust agreements allow other TTPs to sub-contract and provide those additional services. When analysing interworking requirements it should be noted that the legal relationship between a TTP and its subscribers is different from the one between the TTP and non-subscribers (e.g. users who verify digital signatures based on certificates from the CA). Examples of TTPs (CAs) interworking structures can be found in the ITU-T Rec. X.509 | ISO/IEC 9594-8.

6.1 TTP-Users

The means by which a user interacts with a TTP in order to request and receive a TTP service is known as a user interface. Each user may interact with the TTP in different ways depending on what type of service is being offered.

6.2 User-User

After the TTP has completed its tasks, all further communication amongst entities can be done without the assistance of the TTP. The relationship amongst entities as well as the contractual formalisation of this relationship relies very much on their trust in the TTP and the interworking mechanisms of TTPs.

6.3 TTP-TTP

The TTP-to-TTP interface supports secure communications amongst users through the interchange of information concerning the security services provided. In multiple security domains, it is assumed that the TTPs have cross-certified. For example, Figure 4 below illustrates the interfaces used when Entity A asks TTP A for a secret key to communicate with Entity B (1), TTP A transfers the appropriate secret key to Entity A (3) and to TTP B (2) which passes the key to Entity B (3). With this common key, Entities A and B can conduct secure communications (4). As an alternative, using public key technology, Entity A would request secure communications with Entity B from TTP A (1). TTP A would pass Entity A's certificate to TTP B and request Entity B's certificate from TTP B (2). TTP B would pass Entity A's certificate to Entity B (3) and transfer Entity B's certificate to TTP A (2), which would pass it on to Entity A (3). With Entity B's certificate in the possession of Entity A, and vice versa, secure communications could be established between Entities A and B (4).

A large variety of mechanisms may be used for these secure communications exchanges.

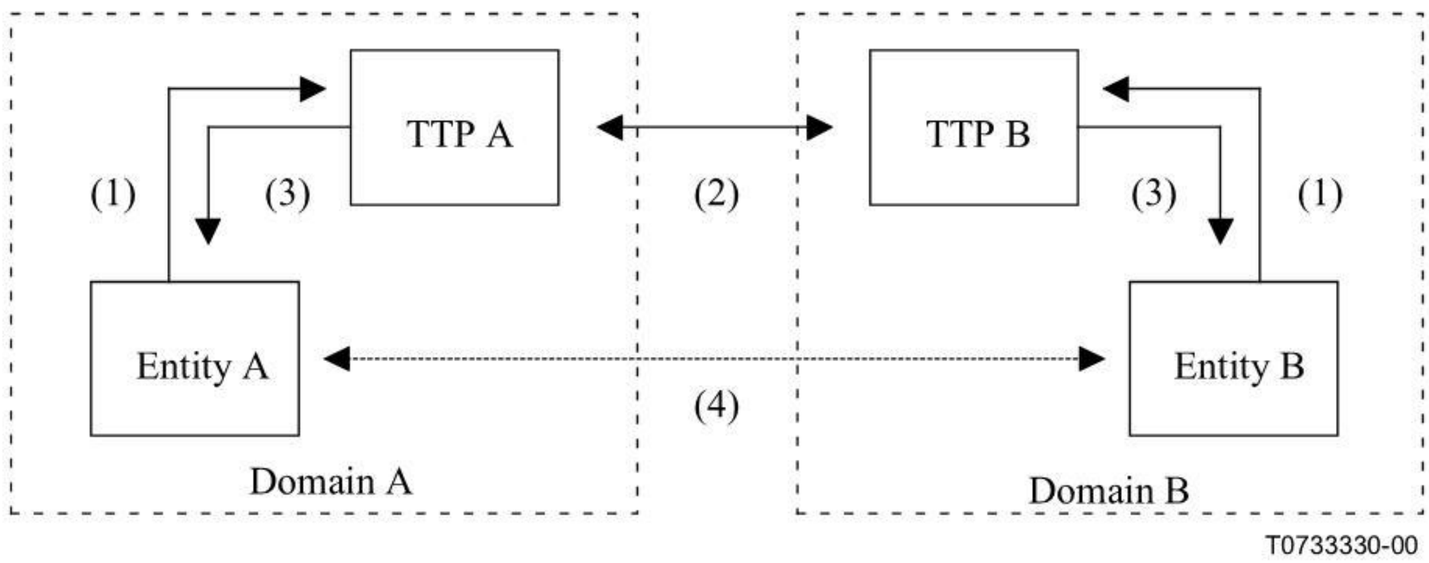

Figure 4 – Interworking of TTPs in Different Domains

NOTE – The mechanisms used are beyond the scope of this Recommendation | Technical Report.

It has to be considered that a given security service may result from the combination of different TTPs offering complementary services with, possibly different levels of security. Therefore, rules have to be established regarding the assessment and rating of the level of security offered by TTPs and methods should be suggested regarding the assessment of the level of security of a multi-TTP service.

The following discussion is relevant in cases where the TTP is a Certification Authority (CA).

CAs can be organised in either hierarchical or non-hierarchical architectures.

In a hierarchical architecture, certification paths have a hierarchy from the root CA to its subordinate CA, respectively following its hierarchical architecture.

In a non-hierarchical architecture, CAs need to cross certify each other to allow a flexible use and exchange of certificates. This cross certification should be done using high assurance levels and a careful code of practice. Once cross certification exists between CAs, validation paths of public key certificates can be constructed. An entity only needs to have trust in the verification key of one CA. This trust then extends via the certification path to the other entity's public key issued by the other CA.

6.4 TTP-Law Enforcement Agency

The primary stated concern of law enforcement authorities and national security agencies is that widespread use of encrypted communications will reduce their capability to fight against crime or prevent criminal and terrorist activities.

Where applicable, in nations with this type of interaction, this interface provides the means by which a law enforcement agency can request and receive from a TTP confidential archived information. This information will enable encrypted communications that were lawfully intercepted, to be decrypted.

7 Major Categories of TTP Services

7.1 Time Stamping Service

A time stamping service seals a digital document by cryptographically binding a trusted time to it (typically to a hash representation of it called "message digest" or "message imprint"), thus providing a means to detect any modification, such as backdating and avoid replay attacks or other forgeries.

Time stamping service relies on the authenticity of the clock that is used, therefore, the TTP needs a time stamping service which uses a clock of very high reliability, availability and trustworthiness.

A message digest may be created using techniques as described in ISO/IEC 10118-1, 10118-2, and 10118-3. Time stamp tokens are described in ISO/IEC 13888-1.

Optionally, the TTP providing time stamping services should register all electronic seals in a chronological order in a permanent archive. Also, a time stamp verification service could be provided.

7.1.1 Time Stamping Authority

A Time Stamp Authority (TSA) is a TTP that creates time stamp tokens in order to indicate that a message existed at a particular point in time.

The TSA provides a "proof-of-existence" for this particular message at an instant in time. A TSA may also be used when a trusted time reference is required and when the local clock available cannot be trusted by all entities. The TSA's role is to time stamp the imprint of a message to establish evidence indicating the time before which the message was generated. For example, the time stamp can then be used:

a) to verify that a digital signature was applied before the certificate was revoked thus allowing a revoked public key certificate to be used for verifying signatures created prior to the time of revocation; or

b) to indicate the time of submission when a deadline is critical; or

c) to indicate the time of transaction.

The TSA should:

a) guarantee only the trusted source of time;

b) include a monotonically (never increasing or never decreasing) incrementing value of the time of day into its time stamp token (the time chosen to be used may be world time[GMT] or local time);

c) produce a time stamp token upon receiving a valid request from the requester;

d) include within each time stamp token an identifier to uniquely indicate the trust and validation policy under which the token was created;

e) time stamp only a hash representation of the message;

f) sign each time stamp token using a key generated exclusively for this purpose and have this property of the key indicated on the corresponding certificate (cryptographic methods other than signing can also be used);

g) include supplementary temporal information (e.g. sports or lottery results) in the time stamp token if asked by the requester; and

h) provide a signed or otherwise verifiably secure receipt in the form of an appropriately defined time stamp token to the requester, where appropriate, as defined by policy.

Detailed information and an example of a time stamping protocol can be found in PKIX Part V, and also in ISO/IEC WD 18014.

7.2 Non-repudiation Services

TTPs may be involved in the provision of non-repudiation services, depending on the mechanisms used and the non-repudiation policy in force. The purpose of non-repudiation, in conformance with ISO/IEC 13888-1, 13888-2 and 13888-3, is to provide verifiable proof or evidence recording of data, based on cryptographic check values generated by using symmetric or asymmetric cryptographic techniques, of approval, sending, origin, submission, transport, receipt, knowledge and delivery. One important component of non-repudiation to provide the verifiable proof is time stamping.

There are two basic approaches that can be used to decide whether or not a TTP is essentially required within the non-repudiation service.

1) In conformance with ISO/IEC 13888-2, non-repudiation services based on symmetric techniques need an:

   a) on-line service for evidence generation, evidence verification, and generation of secure envelopes; and

   b) off-line service for the personalisation of appropriate keys in a trusted cryptographic device, e.g. a Smart Card or a security module.

It is important to note that non-repudiation based on symmetric techniques relies on one single key, which may be used by a TTP in offering a notary service. The use of this key is restricted, and its distribution to entities must be controlled.

2) In conformance with ISO/IEC 13888-3, asymmetric techniques may be specified to establish mechanisms for non-repudiation services of origin, delivery, submission and transport.

If a TTP is not directly involved in the non-repudiation service, other TTP services, such as certified key assignment, with or without key generation, or certificate management services, can be used to set up the necessary infrastructure.

Figure 5 illustrates an example of a TTP providing non-repudiation services for entities A and B.

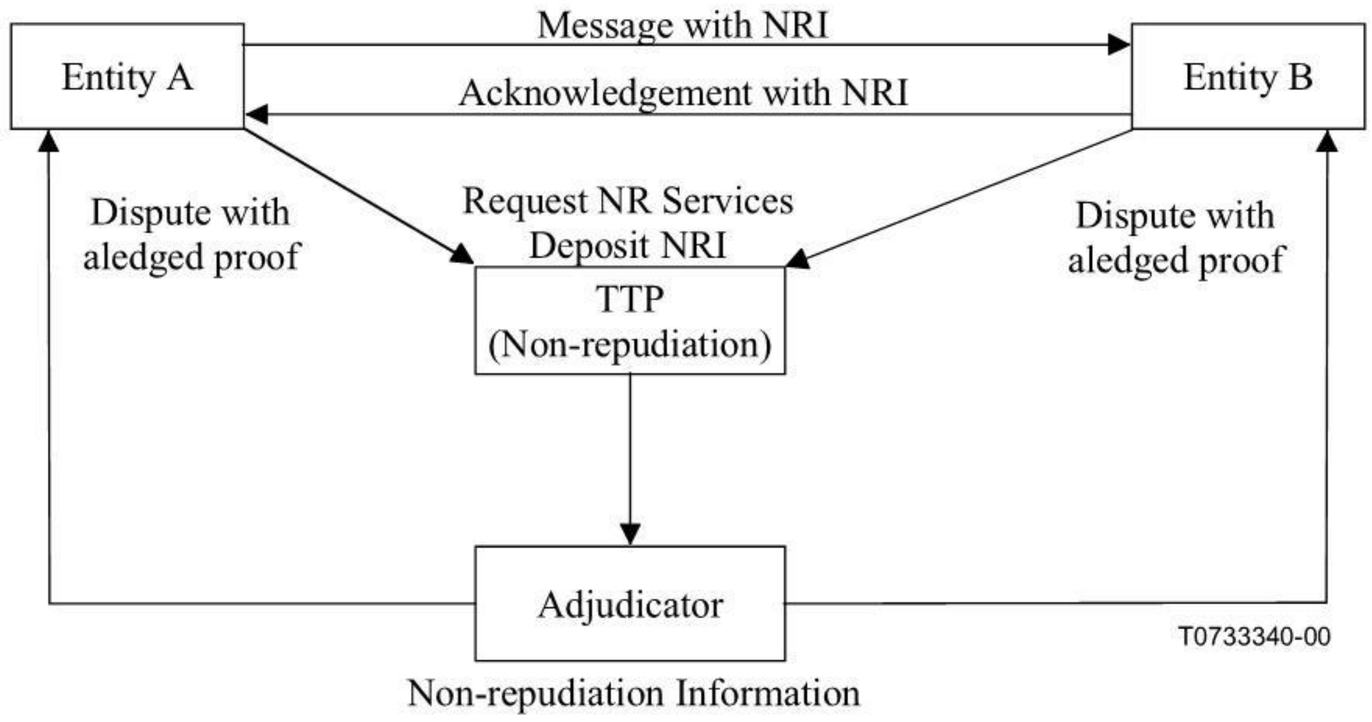

Figure 5 – Example of Non-repudiation Architecture

Additional details on TTP involvement in the provision of non-repudiation services can be found in ISO/IEC 13888-1.

7.3 Key Management Services

In conformance with Key Management standard ISO/IEC 11770-1, key management relies on the basic services of generation, registration, certification, distribution, installation, storage, derivation, archiving, revocation, deregistration and destruction. Other security related services that may be used include access control, auditing, authentication, cryptographic and time stamping services.

An on-line TTP can act as a key management server in support of services using cryptographic techniques. Depending on the way the key material is generated, the service may be a key distribution service (when the key is generated by the TTP) or a key translation service (when the key is generated by one of the entities and transmitted to the other by the TTP).

7.3.1 Key Generation Service

This service is invoked to generate keys in a secure way for a particular cryptographic algorithm. The generation of secret, and unpredictable numbers with certain properties is fundamental for key generation. For example, random numbers can be generated either by a cryptographically secure pseudo random number generator or by a random source such as radioactive decay. The different elements of random numbers include random number generation, random number generation validation, domain parameter generation, domain parameter validation, key pair generation, and public key validation. A useful introduction to random numbers including generation methods is available in RFC 1750.

It is important that the following are considered for both symmetric and asymmetric techniques:

a) possible weak keys for the algorithm; and

b) the usage of the full key space.

7.3.2 Key Registration Service

In this instance the TTP is an accredited registration authority to provide the registration of keys for entities with each registered key associated with a specific entity. This service includes the maintenance of a key register and related information in a suitably secure manner, e.g. a public key register for an entity's public key. The public keys have to be certified by one or more certification authorities. To increase the availability and reliability of this service certified keys should be distributed to multiple public accessible and trustworthy directories, in which case, a periodic update of all directories is necessary to achieve consistency. Services provided by a key registration authority are registration and deregistration. Details on the contents of a key register can be found in ISO/IEC 11770-1, Annex B.

7.3.3 Key Certification Service

In this instance the TTP is an accredited certification authority that creates a key certificate. The certification authority time stamps and signs public keys or attributes to make them valid and authentic in a trusted key infrastructure. Entities using certificates have to trust the same certification authority or at least one common authority within a certification

hierarchy. The certified keys can be generated either by a generation service of the TTP or by the key owner. The service also includes the recertification of expired certificates. Certificates for public keys are discussed in detail in ISO/IEC 11770-1, Annex D.

It is important to note that services of:

1) providing assurance of proof of possession of the private key by the claimed owner; and
2) providing assurance of validity of the value of the candidate public key (and validity of the values of a candidate set of domain parameters, when appropriate),

can be invoked outside of the Certification service, as well as part of a Certification service.

7.3.4 Key Distribution Service

The purpose of a key distribution service is to distribute keys securely to authorised entities. Depending on the TTP's security policy, keys may have to be forwarded to other TTP services, e.g. a directory service. These services could be provided by the same or another TTP. Distribution of keys between TTPs and also between TTPs and entities, especially if distributed through insecure channels, should be protected using cryptographic protocols and mechanisms. Details on different mechanisms to distribute keys between entities can be found in ISO/IEC 11770-2. Details on different mechanisms regarding key agreement of secret keys and transport mechanisms for secret and public keys can be found in ISO/IEC 11770-3. Details on different mechanisms not in ISO/IEC 11770-3 can be found in ISO/IEC 15946-3.

According to ISO/IEC 11770-1 one special occurrence of key distribution is key translation. The role of a key translation service is to translate keys for distribution between entities so that each entity shares a unique key with a Key Translation Centre.

7.3.5 Key Installation Service

This service is always needed before a key can be used as it establishes the key within a key management facility in a manner that protects it from compromise.

7.3.6 Key Storage Service

This service provides secure storage of keys intended for current or short-term use, or for backup, usually in a physically separate location to ensure the confidentiality and integrity of the keys. It is essential that any attempted compromise should be detectable.

7.3.7 Key Derivation Service

This service creates a potentially large number of keys using a secret original key called the derivation key, non-secret variable data and a transformation process. This derivation key needs special protection and the transformation process should be non-reversible and non-predictable to ensure that the compromise of a derived key does not disclose the derivation key or any other derived key. A potentially large number of keys are created by the transformation process by using an original key, called the derivation key, and non-secret variable data.

7.3.8 Key Archiving Service

This service is similar to key storage service, however its purpose is to provide for the secure, long-term storage of keys after normal use is discontinued. The service is intended for keys that may need to be retrieved at a much later date to prove or disprove certain claims.

7.3.9 Key Revocation Service

The purpose of this service is to assure the secure deactivation of a key when the key is known or is suspected of being compromised. A list of revoked keys should be distributed regularly. The revocation can be requested by the key owner, by another authorised person or by a trusted entity if there is any suspicion that the key has been compromised. According to ISO/IEC 11770-1, Annex D, every stop-list entry should include the revocation time, the time of the request and the time of known or suspected compromise. In some cases the revocation may have to meet firm time restrictions, and there should only be a short interval between the time of the request and the distribution of the revocation announcement. A TTP may only be responsible for revoking keys for its clients, usually by informing each client as to which of its keys is revoked.

7.3.10 Key Destruction Service

In this instance the TTP is an accredited registration authority to provide the destruction of keys that are no longer needed. The TTP should first provide a deregistration service to remove the association of a key with its entity. This is followed by the destruction of the key by destroying all information related to the key so that there is no means to recover the destroyed key. This includes the destruction of all copies of archived keys after an investigation to ensure that no archived material protected by these keys will ever be needed again.

7.4 Certificate Management Services

The format of a public key certificate and an attribute certificate is defined in ITU-T Rec. X.509 | ISO/IEC 9594-8. The attribute certificate format is compatible with the X.509 certificate and is not restricted to a specific area of use. This is of importance because it is possible to address the same "subject" (e.g. an entity) with the attributes (e.g. entity name) used in an X.509 (public key) certificate. Additional details regarding certificate management can be found in Annex D of ISO/IEC 11770-1.

The following subclauses describe some certificate management services.

7.4.1 Public Key Certificate Service

A Certification Authority (CA) is a TTP that provides public key certificates and takes care of the information necessary for the revocation of such issued certificates. This is accomplished by verifying the identity of the requester before issuing a public key certificate, which includes a limited validity period. The CA has to make sure that the requester has the knowledge of the private key. The CA may make sure the requester's public key completes a validation test and, if applicable, domain parameter validation tests.

The lifecycle of public key certificates is managed by a TTP providing the services of a CA. The CA is trusted by its users based on the use of adequate cryptographic mechanisms and equipment, and on professional management and control practices. This trust is confirmed by an independent audit function which makes the audit results available to entities. The responsibilities of the CA include:

a) identifying the entities whose public key information is presented for certification; procedures for describing this aspect are given in more detail in B.1, Registration Process Procedures;

b) ensuring the quality of the asymmetric key pair used to produce public key certificates;

c) securing the certification process and the private key used to sign the public key information;

d) managing the system-specific data that are to be included into the public key information, such as the public key certificate serial number, certification authority identification, etc.;

e) assigning and checking of validity periods;

f) advising the entity identified in the public key information that a public key certificate has been issued; the means used to convey this advice should be independent of the method used to convey the public key information to the CA;

g) ensuring that all information included within a certificate meets the requirements of the applicable certificate policy, e.g. by ensuring that two different entities are not assigned the same identity, so that they can be properly distinguished;

h) maintaining and issuing of revocation lists; and

i) logging all steps involved in the public key certificate generation process.

One CA can certify another CA's public key information to provide a public key certificate. Hence, authentication may involve a chain of public key certificates. The first public key certificate in such a chain should be obtained and authenticated by some means other than with public key certificates.

NOTE – As the recipient of a digital signature may have had no prior contact with the CA issuing the certificate accompanying that digital signature, there is a need for a mechanism whereby the recipient can establish a level of trust in the CA. This trust is established through the process of cross certification. Cross certification can be gained by a bilateral agreement between the two CAs, that each or both issue the other a certificate.

Several issues are considered during cross certification, including:

a) identification processes;

b) key generation and storage processes;

c) liability;

d) revocation processes;

e) security processes; and

f) differences in policies and practice statements.

7.4.2 Privilege Attribute Service

Some privilege attributes may change more frequently than other attributes. Therefore, it is anticipated that only attributes that are frequently used, and that are infrequently changed should be included in a public key certificate. Also, a separate data structure (e.g. attribute certificates, tickets, etc.) should be used to "secure" those attributes that are changed often (e.g. credit limit, access privileges, power of representation given by a company, etc.).

Two basic approaches can be employed to "secure" attributes:

1) Tickets – a ticket is a data structure which contains several attributes and which is encrypted by a TTP. Such tickets are used, e.g. within Kerberos (RFC 1510), and could contain an entity's identity, network address, etc.; and

2) Attribute Certificates – an attribute certificate may or may not exist in combination with a public key certificate. They can exist in combination because the public key associated with the public key certificate should be used to prove that an entity is the authentic subject of the attribute certificate.

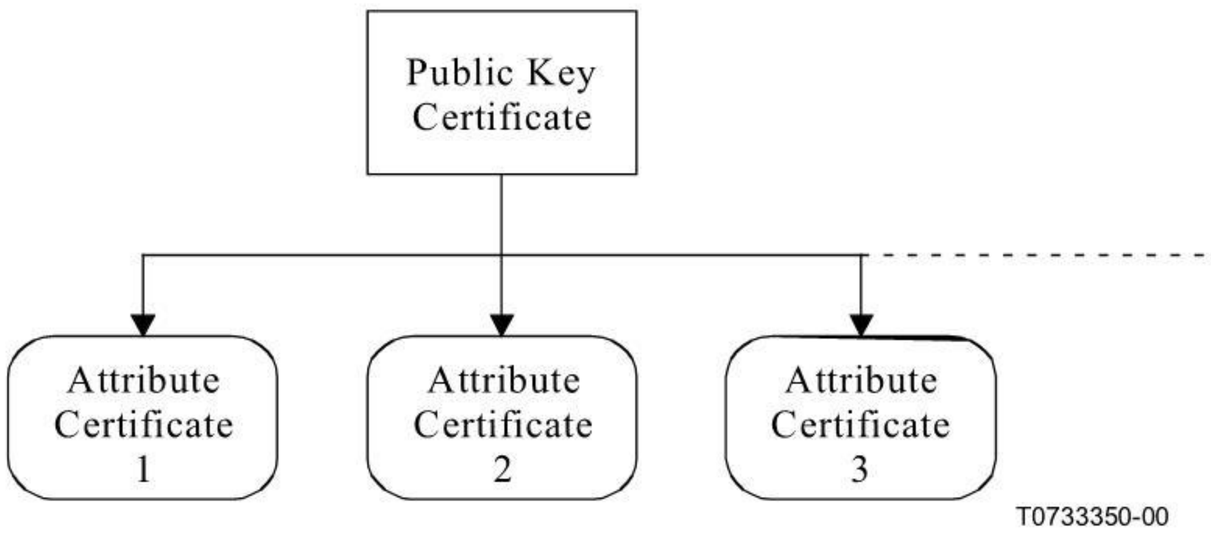

Figure 6 – Link Between an Attribute Certificate and a Public Key Certificate

Figure 6 illustrates the second approach in which an attribute certificate unambiguously refers to a public key certificate. More than one attribute certificate can be linked to a public key certificate. Different attribute certificates could support different areas of use, e.g. personnel related issues (credit limit for electronic commerce), or authority within an organisation.

When assigning only attribute certificates a TTP is acting as an Attribute Authority (AA). In this case the functional links between public key certificates and attribute certificates, as described in Figure 6, will imply appropriate agreements between CA and AA.

7.4.3 On-line Authentication Service Based on Certificates

An on-line authentication TTP process behaves as a certification service for Authentication Certificates; the recoverability of the Authentication Certificates is possible at the next authentication exchange. Such a TTP is commonly known as an Authentication Server.

7.4.4 Revocation of Certificates Service

An entity authorised to revoke a certificate and who wants to revoke its certificate, should contact the CA which issued the certificate to advise that the certificate is no longer valid. After the CA has checked the certificate's status, the CA generates a CRL using the signature of the CA's private key.

A CRL is a digitally signed list that contains the information of revoked certificates generated by the CA, which had issued the certificates.

Each CA must manage the CRL which contains all revoked certificates, and the CRL information must contain a unique serial number and a revoked date of that certificate.

In another approach an on-line TTP can be used as a certificate validation server providing information on the status (including revocation) of an identified certificate.

7.5 Electronic Notary Public Services

Notary public services are high level services that make use of a number of basic services such as time stamping, certification, directory service, digital archiving and non-repudiation. In principle a document will be given to the TTP, and the TTP attests or certifies this document by use of digital signatures or some other means. Part of this service may be a directory service, where the information, such as formerly certified documents, may be retrieved from a database or directory.

A notary public service may attest and certify certain classes of documents, e.g. that a document existed at a certain point in time, in order to give it credibility and authenticity. Such a service may be used for mediation of a dispute between entities and may be authorised by some authority.

The notarisation service works like an electronic public notary. It is able to store time stamped and signed digital documents. (Note that all of these documents have to be registered.)

There are many complex issues in the areas of evidence, notary authority and liability. The issues vary in different jurisdictions, so formal legal advice or review is suggested in these areas.

7.5.1 Evidence Generation Service

Evidence generation consists of the TTP gathering information related to a document, message, or a security related event on a network or system. This can include:

a) the identities of the entities involved;

b) the location of the entities;

c) the data transferred;

d) method of transfer; and

e) time stamping.

Much of this information is typical of what is required to provide an audit trail.

When a TTP collects security related event data on behalf of entities, a similar list of information may be required for analysis and study, and without identifying the originators of the data, share the results with all entities. The details regarding the collection of these data should be described in service level agreements between the participating entities and the TTP.

7.5.2 Evidence Storage Service

In conformance with ISO/IEC 13888-1, evidence storage service is performed in combination with evidence transfer and retrieval services. The evidence stored depends on the security policy in effect.

7.5.3 Arbitration Service

If there is a dispute, and the TTP's dispute resolution mechanisms and procedures fail to resolve the dispute, an adjudicator may be requested to provide arbitration services. The adjudicator is responsible for collecting evidence from disputing parties and then to make a decision which will resolve the dispute.

7.5.4 Notary Authority

A Notary Authority (NA) is a Trusted Third Party that registers data at an instant of time and may also verify the correctness of the specific data that was registered according to some security policy. In its basic role, a NA acts as a recording service, while in its extended role it acts as a validation service. The Notary service may in this way contribute to provide a non-repudiation service. When the Notary performs verification, it will add information to the data that was originally registered. This may allow entities trusting the Notary to make sure that the data has been verified according to the security policy at a given instant in time.

As an example, a Notary may notarise a certificate according to a security policy. In that case, the NA verifies that the certificate included in the request is a valid certificate, according to the security policy, and determines its revocation status at a specified time. Again, it checks the full certification path from the certificate signing entity to a trusted point. The NA may be able to rely on all relevant Certificate Revocation Lists (CRLs) and Attribute Revocation Lists (ARLs), or the NA may need to supplement this with access to more current status information for the CA. It includes this information, along with a trusted time, to create a notary token.

As another example, a Notary may notarise a digital signature according to a security policy. The NA verifies the digital signature and the certification path, according to the security policy. In that case, the validity and revocation status of an entity's public key certificate and/or the validity and the full certification path from the signing entity to a trusted point

(e.g. the NA's CA, or the root CA in a hierarchy) will be checked according to the security policy. The NA may be able to rely on all relevant CRLs and ARLs, or the NA may need to supplement this with access to more current status information from the CA. It includes a trusted time and creates a notary token.

As a final example, a Notary may notarise a formatted data. The NA verifies the correctness of the data and creates a notary token. In this case, however, data "correctness" is not only focused in scope as signature correctness; the particular definition to be applied is therefore necessarily security policy- and datatype-dependent. For example, the data itself may contain one or more signatures (where "correctness" relates to the validity of these signatures), or it may contain assertions (where "correctness" relates to the truth value of these statements), or it may contain a contract (where "correctness" relates to the legal validity of the document).

The Notary Authority may:

a) verify the correctness of the enclosed digital signature using all appropriate status information and public key certificates, and if asked by the requester, produce a signed notary token attesting to the validity of the signature;

b) verify the validity of the enclosed certificate and its revocation status at the specified time using all appropriate status information and public key certificates, and produce a signed notary token attesting to the validity and revocation status of the certificate, if asked by the requester;

c) include a monotonically incrementing value of the time of day or a time stamp token into its notary token;

d) include within each signed notary token an identifier to uniquely determine the trust and validation policy used for this signature;

e) sign each notary token using a key generated exclusively for this purpose and have this property of the key indicated on the corresponding certificate;

f) indicate in the token whether or not the signature or certificate was verified, and if not, the reason the verification failed; and

g) provide a signed receipt (i.e. in the form of an appropriately defined notary token) to the requester, where appropriate, as defined by policy.

More details and an example of a notary protocol can be found in IETF Notary Protocols.

7.6 Electronic Digital Archiving Service

An electronic digital archiving service is a service provided by a document recorder, at which electronic documents are registered for safekeeping and for retention as a permanent record. The archiving of electronic documents in encrypted form may be required in some instances, especially where the data is highly sensitive and requires extra protection.

The basic operations of an archival service are:

a) storage of documents – the TTP may keep a dated version of the documents in a secure storage location for a fixed period of time; and

b) issue copies of documents – the archiving service will, upon request by an authorised entity, issue a signed copy of recorded documents including the date of registration.

The authenticity of recorded documents depends primarily on cryptographic techniques such as digital signatures.

Long term electronic archiving of documents, e.g. for legislative and lawful reasons (several years), has to take into account four basic issues:

a) the archiving medium might need a regular refresh, e.g. magnetic tape, CD-ROMs, etc.;

b) the technical equipment for accessing archived data may not have a sufficiently long enough life span to continue to provide access to archived data over the full period of time for which access should be possible. The change of equipment will lead to a backup and transfer of archived information to new media;

c) to interpret a retrieved document correctly, it might also be necessary to provide additional information such as the document's data format (e.g. ASCII, Postscript, and HTML), file name and creation date. Further, software is needed that will work with those data formats; and

d) cryptographic algorithms may not have sufficient strength to withstand attack over the archive period; in such cases alternative security techniques (e.g. physical security) are needed.

Archival service can also be used (from an operational requirement perspective) by an organisation for document recovery.

One aspect of archival service is an escrowing service which holds in trust electronic documents for a defined time frame. A document should not be delivered to other entities until certain conditions are fulfilled. The security policy should state under which circumstances an entity may get access to those documents, including legislative or lawful interception (where applicable), and user/business access. A TTP is expected to keep a list of all escrowed documents in chronological order.

For example, if entities A and B have a contractual agreement that requires entity A to give program source code to a TTP to hold in trust in the event that entity A is no longer able to support or maintain the program. At a later date entity B can obtain the program source code from the TTP to support business functions if they are affected.

7.7 Other Services

There are several additional services which may be provided by a TTP.

7.7.1 Directory Service

In many cases, security services rely on actual and trustworthy information, e.g. public key certificates, certification revocation lists, attribute certificates, or an extract from an electronic business register provided by a directory.

Before a directory service can be established the objects under consideration have to be identified by giving them a name. To identify an object unambiguously, the name, or at least the set of objects to be addressed, must be unique.

One option is to apply the OSI naming and addressing standard ITU-T Rec. X.650 | ISO/IEC 7498-3. An example for a directory service and its corresponding access protocols is illustrated in ITU-T X.500-series Recommendations | ISO/IEC 9594. After proper access a directory service allows entities to query information from a database (a collection of data stored permanently on some form of storage media).

An overall view of a directory service architecture is illustrated in Figure 7. After login and successful authentication, each query to request data from the directory is mediated by the Authorisation System. If the entity's access rights are in compliance with the authorisation rules, access will be given. Otherwise, an error message can be sent to the entity. Unsuccessful access attempts, e.g. failed authentication, should result in a log file entry.

The Request Manager handles authorised queries. Its task is to compile the query, access the database, and deliver the response to the entity. It is not necessary for all information to be located at one local database.

The following roles are involved in the security management of a directory service:

a) the security administrator is responsible for the definition of authorisation rules according to the security policy; the range of possible authorisation rules is wide, e.g. the directory service can be publicly available, or restricted to a closed user group which is willing to pay for the service;

b) the auditor reviews the log file periodically in order to detect security violations or intruders; and

c) the database administrator is responsible for maintaining that part of the directory which contains security relevant information. This agent has access rights and can read, write, and remove information from the database.

Information from the directory can be retrieved by different means:

a) Off-line Access: this method provides automatic distribution to subscribers from time to time; the time frame should define when the next update is expected; and

b) On-line Access: this method provides distribution on request by entities; a typical example is an X.500 directory.

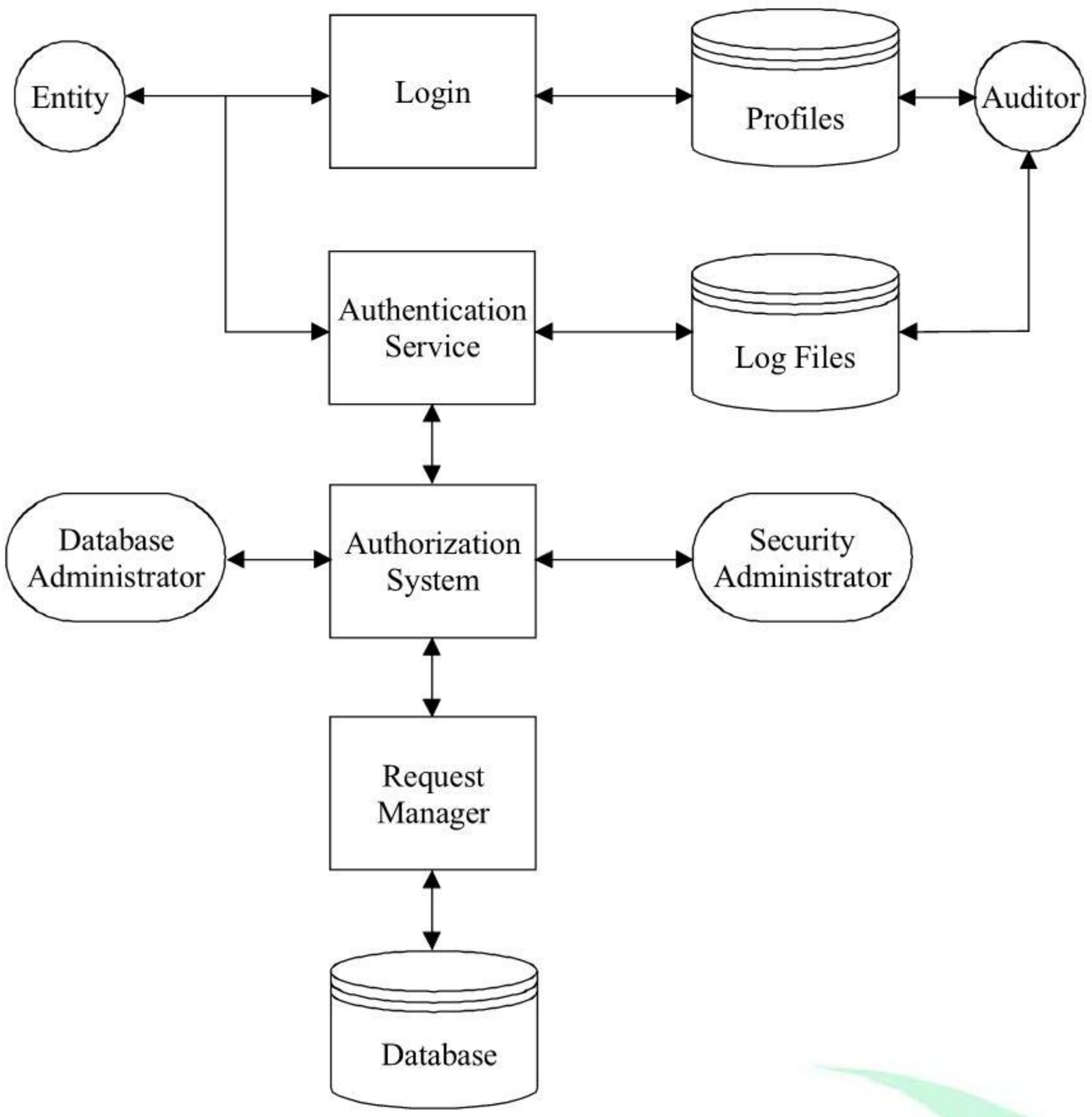

Figure 7 – Directory Service Architecture

7.7.2 Identification and Authentication Service

In a typical scenario, where a distributed architecture consists of clients and distributed or centralised servers, an entity gets access to a server from a local workstation (client). In this environment security can be provided by using an authentication service that is supported by a TTP.

This service could include the initialisation and maintenance of an authentication service, as well as the operation of necessary equipment such as an authentication server. This service can be on-line or off-line. Refer to ISO/IEC 9798 for details about authentication techniques. Further security requirements have to be considered, e.g. the protection of entities from masquerade, data integrity, data origin authenticity, and mutual authentication between entities.

The authentication service can include the authentication of entities (users) or the authentication of data. In most of the cases an on-line availability of this service is needed. The service can provide the verification of certificates or signatures, it can use a cryptographic authentication protocol or a message authentication code (MAC) to provide proof of origin or proof of delivery of data.

The most common implementation of an authentication service is the Kerberos system's ticket granting service. (For additional information refer to Steiner *et al.*: Kerberos: an authentication service for open network systems in the proceeding winter 1988 USENIX Conference, p. 191-202.)

7.7.2.1 On-line Authentication Service

When a large number of entities need to communicate, a peer to peer authentication service may use a TTP in order to avoid each entity having to be in possession of authentication information for all entities. The on-line TTP is involved in every authentication operation. The TTP may authenticate entity A and provide it with a certificate to be presented to entity B, or it may verify entity A authentication information received by entity B on its behalf.

Symmetric authentication schemes require that each entity, which wishes to be authenticated, should share a secret key with every other entity. Instead of generating and distributing a large number of keys [n(n-1)/2 keys for a group of n entities] an on-line authentication service could be used to reduce the number of keys. The result is that:

a) only the TTP providing the authentication service would share a secret key with every entity; and

b) each entity would share a secret key with the TTP.

Two general approaches can be employed:

a) a token based approach. Before the entity is able to authenticate itself, the entity may request a token from a TTP. This token is used in the authentication procedure as described in more detail below; and

b) the entity that wishes to be authenticated sends a sealed message, directly, because the verifier has no means (no common key) to validate this message, the TTP processes this on behalf of the verifier, and notifies him about the result.

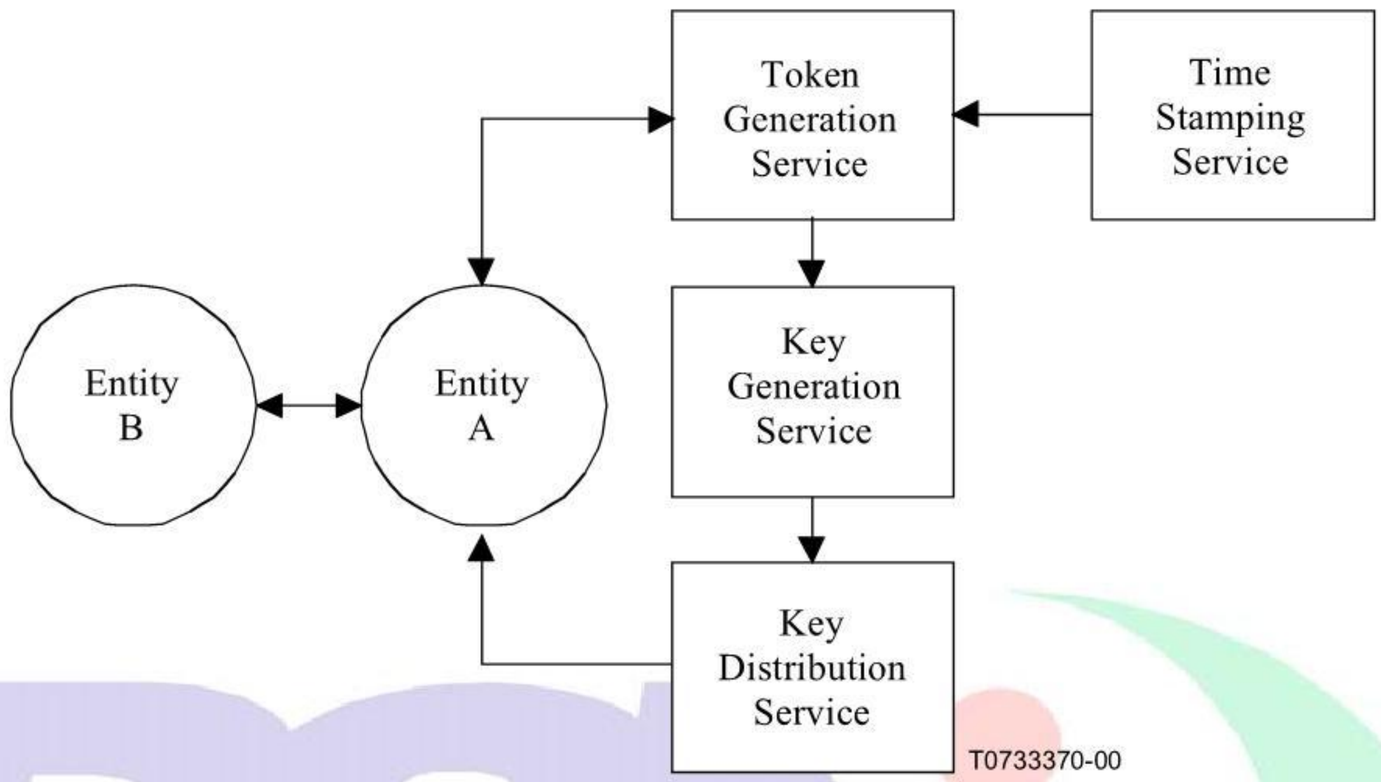

Figure 8 – Example for On-line Authentication Services

A general model for an on-line authentication service is illustrated in Figure 8. Such a service can be divided into two phases:

a) Initialisation Phase: During this phase the main tasks could be the proper identification of entities, and the provision of keying material; and

b) Operation Phase: It is assumed that the user, entity A, has to authenticate itself to a local TTP providing authentication services. This service provides entity A with the necessary credentials to gain access to the remote user, entity B.

In principle, this service is carried out using several steps, and each step can consist of more than one message exchange. If entity A wishes to access an application or service provided by entity B, then entity A might go through steps 1 and 2:

1) Entity A sends a request to the authentication service provider together with its means for authentication (e.g. password, or authentication token generated by using a smart card), requesting credentials.

2) The authentication service provider verifies entity A's access rights, and if the conditions are fulfilled, the response shall be a token, which enables the entity to authenticate itself, to gain access for the requested server or application at entity B's site. The token can contain a time stamp, session key, cryptographic material for authentication and optionally, other material.

Steps 3 and 4 do not involve the authentication service provider directly. But the token which grants entity A access to entity B's services has to be chosen according to the keying material which is shared by the authentication service provider and entity B.

3) The token is sent from entity A to a remote entity B, which verifies the received token. This token should have been chosen according to the keying material which is shared by entity B and the authentication service provider. If it matches, entity B will grant access to the required service.

4) Optionally, if mutual authentication is required, entity B should authenticate itself against entity A in the same secure fashion that entity A had done previously.

An example for such an authentication service is provided in RFC 1510.

7.7.2.2 Off-line Authentication Service

Off-line authentication services rely primarily on asymmetric techniques in combination with certificate management services.

The off-line TTP generates and distributes in advance, off-line authentication certificates which entity B can later use to validate an authentication exchange. This authentication certificate can be stored in advance by entity B, or sent together with Authentication Information (AI) by entity A at the time the authentication takes place. It can also be stored in a repository where entity B can retrieve it when necessary.

Off-line authentication using a TTP is commonly associated with the concept of Certification Authorities. Additional details can be found in ISO/IEC 9798-1 and ISO/IEC 11770-1.

7.7.2.3 In-line Authentication Service

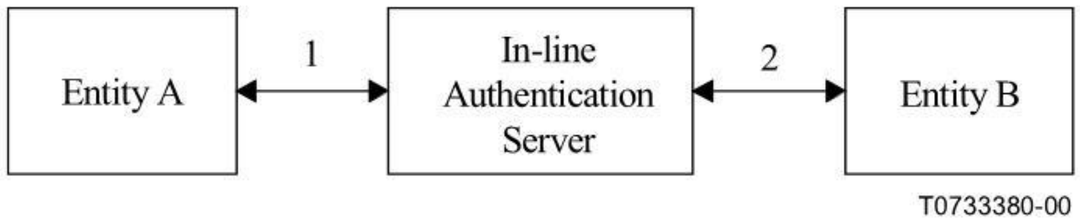

Figure 9 – Example for In-line TTP Authentication Service

In this example, the TTP authentication server is positioned in the communication path between both entities as illustrated in Figure 9. The authentication process is split into two steps, and each step could consist of more than one message exchange.

First, entity A attempts to authenticate itself to a TTP. Second, if entity A's authentication is successful, the TTP authenticates itself to entity B and vouches the identity of entity A including an authentication between the TTP and entity B.

7.7.3 In-line Translation Service

When the two entities belong to different security policy domains, the TTP has to translate the authentication policy of the target domain into that of the originating domain, e.g. in terms of strength of the authentication mechanism to be employed. This scheme may also consist of a chain of TTPs linking the two entities.

7.7.4 Recovery Services

These services are optional and not commonly offered as separate services but in combination with other services that may be offered as part of doing day to day business.

7.7.4.1 Key Recovery Services

Key recovery, key escrow and key encapsulation are functions of a cryptographic system that provide a backup decryption capability, allowing authorised entities under certain conditions to decrypt data using information supplied by one or more TTPs. ("Trusted" in this context is used to mean trusted by both the user and the authorised entity.)

The term Key Recovery is used in different ways depending on the context in which it is applied. For example, it is used in some contexts as a generic term covering both escrow and/or encapsulation systems. In another context it is used as a replacement term for escrow and/or encapsulation.

- ∞ Key Escrow: In a cryptographic system using key escrow, a copy of a secret key, or the means to generate it, is either held by an authorised TTP or may be split into two or more parts that are held by authorised TTPs. In accordance with national law, the TTPs would make such keys or key parts available to authorised entities.

- ∞ Key Encapsulation: In a cryptographic system using key encapsulation, parameters to reconstruct the key are either (a) appended to encrypted data or (b) logically associated with the encrypted data but carried or stored in a separate physical location. In accordance with national law, the cryptographic system would allow a third party to rebuild a key on request with help of information supplied by one or more authorised TTPs. With key encapsulation, the TTPs do not hold the key or key parts directly, but essential information needed in the reconstruction process.

NOTE – The differences between the various schemes depend essentially on implementation details, the infrastructure (i.e. the functions and liabilities assigned to the TTPs) and the institutional arrangements set by national law. In any scheme, once a copy of a secret key is reconstructed or handed over to a third party, this key can no longer be regarded as secret. For example, all communications and stored data encrypted with this key could eventually be decrypted. Key Recovery, Escrow and Encapsulation should only be used for confidentiality keys.

Key recovery services enable data to be decrypted whether it is data being communicated or in storage. Typical areas of application include those of lawful interception (where applicable), and user/business access. The main difference between these areas of application are the prescribed conditions under which decryption of ciphertext can take place.

For example, an organisation may choose to operate a recovery service to provide keys to recover a company's business files and information that have been encrypted by employees. The keys are employed for emergency decryption to recover data encrypted by keys that have been lost or damaged.

There is a requirement for strong access control mechanisms, with only authorised, identified and authenticated people with a "need-to-know" able to gain access to keys. To increase the trustworthiness and reliability of keys, they could be stored in encrypted form or distributed to more than one location.

When providing key recovery services a TTP might combine the roles of a key generation and/or distribution agent for its users, as well as a supplier of user keys. A TTP operating such services will also need to deal with issues such as key revocation, storage, retrieval and reconstruction.

7.7.4.2 Data Recovery Services

This service may be fulfilled using one of two types of basic schemes:

The first type of scheme is characterised by private or secret keys associated with entities being deposited with one or more TTPs before data is encrypted for communication or storage. This key information can be used according to contractual and legislative requirements at a later time to recover data.

The second type of scheme is characterised by an individual using public key material related to one or more TTPs for encrypting data for the purpose of communication and storage. The encryption procedure allows for decryption by the intended recipient. It also allows for recovery of the data according to contractual and legislative requirements using private key material, held by one or more TTPs, and information associated with the encrypted data.

7.7.5 Personalisation Service

The personalisation service includes the encryption of secure cryptographic material in security tokens, e.g. smart cards. The cryptographic material encloses among others secret keys, public keys, certificates and random numbers. They have to be written into a tamper resistant environment, readable only by the intended, identified and authenticated entities. A registration of the personalised token and the authorised owners should be provided by this service.

7.7.6 Access Control Service

An on-line TTP is able to provide access control information in the same manner it provides authentication information when requested by an authorised entity. It acts as a certification service for access control "privileges" of an entity to ensure that the resources of a key management system can be accessed only by authorised entities in an authorised manner. Details can be found in ISO/IEC 11770-1. An on-line access control TTP is known as an Access Control Server.

7.7.7 Incident Reporting and Alert Management Service

According to ISO/IEC TR 13335, an IT security policy has to be reviewed regularly and kept up-to-date in response to a fast changing environment. There should be procedures to deal with specific security events detected by, or brought to the attention of the TTP that is providing the incident reporting and alert management services. This service may be processed manually or automatically.

If an incident such as fraud occurs, the detailed information about this incident is reported to the entity responsible for reported incidents, or, that entity detects an incident by itself:

a) either of the entities could send an alert message to a TTP; or

b) a TTP could receive event information automatically, e.g. by tracing communication; or by requesting information from other entities, e.g. detection as a result of the loss of availability.

Such an incident causes an impact for the relevant organisation, and requires analysis and study, with resolutions that will prevent or reduce the impact of a recurrence of the incident.

When an entity reports an incident to its TTP, the TTP should provide alert management services to other entities as provided by their service level agreements.

Additionally, all relevant event information (occurrence, impact and actions) should be made available for further analysis and study. As a result of alert information, management actions could be, e.g. the transmission of alert messages to other entities, and possibly to other TTPs. One reason may be that a Certification Authority's private key, or an entity's private (secret) key is compromised.

There are instances where entities would like to share, and have access to, aggregated information about security-related threats, vulnerabilities, incidents and events in their business sector. However, these entities are reluctant to share information when it may reflect an exposure in their security system or reduce the level of their client's trust. A TTP can provide a service among entities where information is aggregated, analysed and shared with other entities in accordance with the level of service agreements that are in place. Figure 10 illustrates an example of a TTP that can collect security related incident information from one entity and then without identifying the entity, share that information with all other entities. The TTP can also collect information from all entities for analysis and then share the results with all entities.

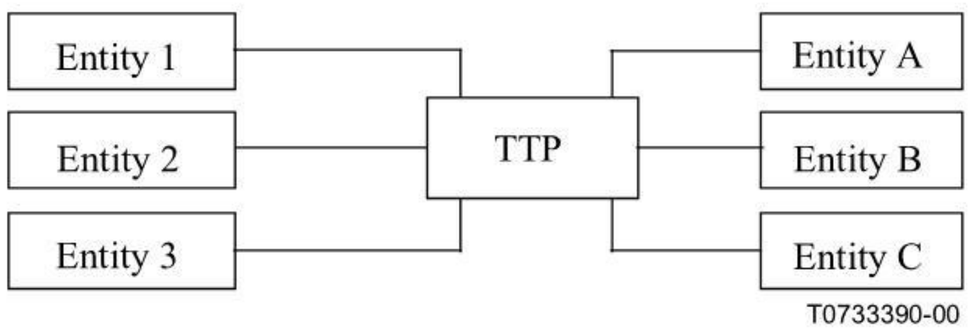

Figure 10 – Example of Alert Management Service

Annex A

Security Requirements for Management of TTPs

(This annex does not form an integral part of this Recommendation ⌋ Technical Report)

In practice, an assessment should be carried out to identify the level of risk associated with the TTP services to be implemented. The type and strength of security requirements to be selected will depend on the specific services provided by the TTP as well as on the risks involved in case the TTP services should become compromised. The security requirements associated with these identified risks should be specified in the TTP's security policy. This assessment and policy development should include the following:

a) users, administrators and operating personnel of the TTP should only have access to information and resources they are entitled to;

b) the administrative procedures should ensure the unique and secure identification, and registration of users and operators of the TTP services;

c) highly sensitive information, which is fundamental for the trust in the TTP, such as the private key of a Certification Authority (CA) or the top-level key of a Key Distribution centre, should be generated, installed and managed by well-documented and trustworthy procedures;

d) in order to ensure the traceability of operations and transactions and the accountability of entities, the following measures should be taken with the required strength:

   1) authentication of entities;

   2) electronic signature of all security sensitive requests, transactions and operations; and

   3) restrict auditing data to the proper authorities (e.g. security auditors).

e) in order to protect the privacy and business interests of all the involved entities, information at interfaces, carried by protocols and on storage media, should have the required level of integrity and confidentiality protection;

f) system security, including operating system security, of all components governed by the security policy of the TTP should provide the necessary protection in the actual operating environment;

g) adequate security management should cover the initiation, monitoring and control of the security services protecting the services provided by the TTP;

h) procedures should be available to recover to a secure state in case of a security breach. This also implies the recovery or replacement of top-level secret key(s) of the TTP;

i) mechanisms should be in place to safeguard against any single point of vulnerability that might exist in systems where a TTP is able to recover the encrypted data by using key recovery;

j) if required by the security policy of the entities involved, the TTP should provide the means to ensure that only keys needed by an authorised entity can be recovered by the TTP; and

k) recovery procedures should also include minimising the impact to the entity through appropriate notification procedures.

Annex B

Aspects of CA management

(This annex does not form an integral part of this Recommendation | Technical Report)

B.1 Example of Registration Process Procedures

The CA is responsible to undertake the procedures stated in order to establish that the applicant of a certificate is the person that he/she claims to be. Under given circumstances the CA can authorise another entity named Registration Authority (RA) to perform the process of subscriber's registration on behalf of the CA.

The subscriber enrolment process may be initiated by the applicant (the person applying to become a subscriber), the CA, an RA, or an organisational officer who is coordinating establishment of an organisational network.

The CA (RA) should verify that each certificate applicant has a right to obtain that certificate and, if the certificate implies that the subscriber has particular attributes or privileges, then the applicant has the corresponding attributes or privileges.

A subscriber's relation with an employer and the employer's approval of issuing a certificate for the subscriber has to be certified by a legitimate representative of the employing organisation.

In its agreement with the employer, the CA should ensure that the employing organisation undertakes the responsibility to inform the CA about relevant changes in the state of employment during the validity period of issued certificates.

The applicant needs to personally present himself or herself to a CA, RA or an appointed representative of the CA, to be authenticated prior to certificate issuance. This is regardless of whether the subscriber is independent or associated with an employer. This can be handled directly by the employer only if the employer itself is a CA or an RA appointed by the CA.

The applicant should present valid identification papers. Indication of the means of identification should be given on the application form, and the person in charge at the CA, or his representative RA, has to personally sign that the verification actually has been performed.

When authenticating an applicant, the subscriber should present to the CA or RA a certified and commonly recognised picture-type identification card such as a national identity card.

If the applicant does not possess a picture-type identification as stated above, this can be replaced with a government paper certifying the existence of the claimed identity in combination with an independent individual of full age, which is authenticated as described above, who certify that the applicant has the claimed identity.

Presented details of the individual, such as unique identifiers, name and registered address, should be compared with information in an official register, or another organisational or third party register, that is trusted for this purpose by the CA.

B.2 An example of requirements for Certification Authorities

A Certification Authority (CA) that issues certificates must operate in accord with an appropriate certificate policy. The policy should as a minimum undertake to:

a) provide certification and repository services that are consistent with each other;

b) provide controls regarding operational requirements;

c) perform the authentication procedures regarding initial registration and revocation requests;

d) issue certificates in accordance with the certificate policy definition and honour the various representations to subscribers and to relying parties presented in a published CPS – Certification Practice Statement (a statement of the practices which a certification authority employs in issuing certificates);

e) support the rights of the subscribers and relying parties who use certificates in accordance with applicable laws and regulations;

f) revoke certificates and issue CRLs of the certificate policy definition (provision of certificate suspension is at the option of the certification authority); and

g) comply with all provisions of its certificate policy definition and any legal provisions in a published CPS.

The CA is responsible for all undertakings listed above, regardless of whether they are performed by the CA or a Registration Authority (RA) appointed by the CA. CA undertakings against all external entities therefore include all RA undertakings.

CAs must provide the following additional undertakings concerning:

a) *Protection of the issuing CA's private key*

A CA should protect its private key in accordance with certain provisions described in the certificate policy definition.

b) *Restrictions on the use of the issuing CA's private key*

A CA's private key used for issuing certificates that conform to this certificate policy should be used only for signing certificates and, optionally, CRLs and other adequate information consistent with the certificate issuance.

If a CA undertakes to act in accordance with other policies, using the same private key or issuing identity, these should be identified in the CPS.

An RA is an entity who is responsible for identification and authentication of entities of public key certificates, but is not a CA or AA, and hence does not sign or issue certificates. An RA may assist in the certificate application process, revocation process, or both. The RA does not need to be a separate body, but can be part of the CA.

Responsibilities that could be allocated to an RA include:

a) validate the identity of the entity requesting a public key certificate, according to the CA's Certification Practice Statement (CPS);

b) validate that the identity of the entity requesting the certificate is the entity certified in the certificate. This may be accomplished by having the entity sign the request for the certificate and having the RA validate that signature using the public key presented for certification;

c) register authenticated entities securely;

d) notify the entity identified in the certificate confirming successful registration and that a certificate has been issued;

e) keep audit records supporting the certificates it issues for the length of time determined by requirements for retention of records;

f) provide guidance to its subscribers on the secure management of the subscriber's private key;

g) use any appropriate means to ascertain that the entity identified in the certificate understands it's responsibilities and is able to comply with them;

h) inform the entities in the domain when the CA's private key has been compromised;

i) handle certificate revocation requests from entities;

j) inform the entity identified in the certificate that the integrity of its operation will be considered compromised if its private key is ever revealed to or used by any unauthorised entity; and

k) maintain sound management and control practices that are to be confirmed by security quality assurance processes and procedures, and independent compliance audits.

An RA involved in practices related to certificate issuance should as a minimum undertake to:

a) provide the controls regarding operational requirements of the certificate policy definition;

b) perform authentication procedures according to rules set forth in the certificate policy definition;

c) perform contracted undertakings and support the rights of the subscribers and relying parties who use certificates in accordance with applicable federal, state, and provincial laws and regulations; and

d) comply with all provisions concerning liability, financial responsibility, fees, publications and repository, compliance audit, confidentiality, intellectual property rights, contractual agreements defined in the certificate policy definition and any legal provisions in a published CPS.

In addition RAs may be required by law to make other warranties.

RAs must provide the following additional undertakings concerning:

a) protection of its private key in accordance with the provisions of the certificate policy;

b) private keys used for purposes associated with its RA function should not be used for any other purpose without the express permission of the CA; and

c) usage of RA private keys should be restricted according to key usage stipulations in their associated certificates.

The Subscriber has also some obligations, which should be covered in the agreement between the CA and the subscriber according to contractual agreements, including:

a) the subscriber should undertake to follow the certain procedures when applying for a certificate;

b) the subscriber should retain control of its private key, protect it in accordance with applicable parts of the certificate policy definition, and take reasonable precautions to prevent its loss, disclosure to any other party, modification, or unauthorised use;

c) the subscriber should report to the CA upon any suspicion that the key may have been compromised;

d) the cryptographic token, on which private keys are stored, should be protected to an extent comparable with that of valuable personal items such as credit cards or a driver's license. The PIN or password used to unlock the token must never be stored in the same location as the token itself; and

e) subscribers should not leave their cryptographic token unattended in an unlocked state (i.e. unattended in a workstation when the PIN or password has been entered).

B.3 Certification Policy and Certification Practice Statement (CPS)

When a certification authority issues a certificate, it is providing a statement to a certificate user (i.e. a relying party) that a particular public key is bound to a particular entity (the certificate subject). However, the extent to which the certificate user should rely on the CA statement needs to be assessed by the certificate user. Different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

The ITU-T Rec. X.509 | ISO/IEC 9594-8 defines a certificate policy as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements". An X.509 Version 3 certificate may contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose.

A certificate policy, which needs to be recognised by both the issuer and user of a certificate, is represented in a certificate by a unique, registered Object Identifier. The registration process follows the procedures specified in ITU-T Recommendations | International Standards. The party that registers the Object Identifier also publishes a textual specification of the certificate policy for examination by certificate users. Any one certificate will typically declare a single certificate policy or, possibly, be issued consistent with a small number of different policies.

Certificate policies also constitute a basis for cross certification of CAs along with a Certification Practice Statement (CPS). Each CA is certified against one or more certificate policies which it is recognised as implementing. When one CA issues a CA-certificate for another CA, the issuing CA must assess the set of certificate policies for which it trusts the subject CA (such assessment may be based upon certification with respect to the certificate policies involved). The assessed set of certificate policies is then indicated by the issuing CA in the CA-certificate. The X.509 certification path processing logic employs these certificate policy indications in its well-defined trust model. The concepts of certificate policy and CPS come from different sources and were developed for different reasons. However, their interrelationship is important.

A CPS is a detailed statement by a CA as to its practices, that potentially needs to be understood and consulted by subscribers and certificate users (relying parties). Although the level of detail may vary among CPSs, they will generally be more detailed than certificate policy definitions. Indeed, CPSs may be quite comprehensive, robust documents providing a description of the precise service offerings, detailed procedures of the life-cycle management of certificates, and more – a level of detail which weds the CPS to a particular (proprietary) implementation of a service offering.

The detail in a CPS is necessary to make a full assessment of trustworthiness in the absence of accreditation or other recognized quality metrics. A detailed CPS does not alone however, form a suitable basis for interoperability between CAs operated by different organisations. Rather, certificate policies best serve as the vehicle for relying parties to determine whether a particular certificate is suitable for their application/purpose. A CA with a single CPS may support multiple certificate policies (used for different application purposes and/or by different certificate user communities). Also, multiple different CAs, with non-identical CPSs, may support the same certificate policy.

Refer also to RFC 2527, Certificate Policy and Certification Practices Framework, S. Chokhani, W.Ford, March 1999.

Annex C

Bibliography

(This annex does not form an integral of this Recommendation | Technical Report)

Informative References

- AS/NZS 4444, Australian / New Zealand Standard Code of Practice.
- BS 7799, British Standard Code of Practice – Revision 1, 1999.
- ETSI EG/SEC-003000, *Requirements for Trusted Third Party Services* (Edition 1), Version 7.0, July 1997.
- FIPS PUB 140-1, Federal Information Processing Standard Publication 140-1, Security Requirements for Cryptographic Modules, *U.S. Department of commerce, National Institute of Standards and Technology, January 1994*.
- ISO/IEC Guide 61:1996, *General requirements for assessment and accreditation of certification / registration bodies.*
- ISO/IEC Guide 65:1996, *General requirements for bodies operating product certification systems.*
- ISO/IEC 9798-2:1999, *Information technology – Security techniques – Entity authentication – Part 2: Mechanisms using symmetric encipherment algorithms.*
- ISO/IEC 9798-3:1998, *Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques.*
- ISO/IEC 9798-4:1999, *Information technology – Security techniques – Entity authentication – Part 4: Mechanisms using a cryptographic check function.*
- ISO/IEC 10118-1:2000, *Information technology – Security techniques – Hash-functions – Part 1: General.*
- ISO/IEC 10118-2:2000, *Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher.*
- ISO/IEC 10118-3:1998, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions.*
- ISO/IEC 13888-1:1997, *Information technology – Security techniques – Non-repudiation – Part 1: General.*
- ISO/IEC 13888-3:1997, *Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques.*
- ISO/IEC 15408-1:1999, *Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model.*
- ISO/IEC 15408-2:1999, *Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements.*
- ISO/IEC 15408-3:1999, *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements.*
- ISO TC68 SC2 15782-1, *Banking – Certificate Management Part 1: Public Key Certificates.*
- ISO/IEC 15945, *Information technology – Security techniques – Specification of TTP services to support the application of digital signatures.*
- ISO/IEC 15946-3, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment.*
- ITU-T Recommendation X.520 (2001) | ISO/IEC 9594-6:2001, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types.*
- ITU-T Recommendation X.650 (1996) | ISO/IEC 7498-3:1997, *Information technology – Basic Reference Model: Naming and addressing.*
- ITU-T Recommendation X.680 (1997) | ISO/IEC 8824-1:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation.*

– ITU-T Recommendation X.681 (1997) | ISO/IEC 8824-2:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification.*

– ITU-T Recommendation X.682 (1997) | ISO/IEC 8824-3:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification.*

– ITU-T Recommendation X.683 (1997) | ISO/IEC 8824-4:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications.*

– ITU-T Recommendation X.811 (1995) ⌋ ISO/IEC 10181-2: 1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*

– ITU-T Recommendation X.812 (1995) ⌋ ISO/IEC 10181-3: 1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*

– ITU-T Recommendation X.814 (1995) ⌋ ISO/IEC 10181-5: 1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Confidentiality framework.*

– ITU-T Recommendation X.815 (1995) ⌋ ISO/IEC 10181-6: 1996, *Information Technology – Open Systems Interconnection – Security frameworks for open systems: Integrity framework.*

– ITSEC, *Information Technology Security Evaluation Criteria (ITSEC)*, Harmonised Criteria of France, Germany, the Netherlands, the United Kingdom, Version 1.2, June 1992.

– NIST, *Computer Security Handbook.*

– NIST, *Minimum Interoperability Specification for PKI Components (MISPC)*, 1997.

– PKIX Part V, Internet X.509 Public Key Infrastructure, Internet Draft, Time Stamp Protocols, C. Adams, P. Cain, D. Pinkas, R. Zuccherato, March 2000 (work in progress).

– PKIX Part VI, Internet X.509 Public Key Infrastructure, Internet Draft, Data Certification Server Protocols, C. Adams, Sylvester, Zolotarev, R. Zuccherato, March 2000 (work in progress).

– RFC 1421, *Privacy Enhancement for Internet Electronic Mail: Part 1: Message Encryption and Authentication Procedures*, February 1993.

– RFC 1422, *Privacy Enhancement for Internet Electronic Mail: Part 2: Certificate-Based Key Management*, February 1993.

– RFC 1423, *Privacy Enhancement for Internet Electronic Mail: Part 3: Algorithms, Modes, and Identifiers*, February 1993.

– RFC 1424, *Privacy Enhancement for Internet Electronic Mail: Part 4: Key Certification and Related Services*, February 1993.

– RFC 1510, *The Kerberos Network Authentication Service*, September 1993.

– RFC 1750, *Randomness Recommendations for Security*, December 1994.

– RFC 2459, *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, January 1999.

– RFC 2510, *Internet X.509 Public Key Infrastructure Certificate Management Protocols*, March 1999.

– RFC 2527, *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*, March 1999.

– RFC 2559, *Internet X.509 Public Key Infrastructure Operational Protocols – LDAPv2*, April 1999.

– S2101/02, *Report to the Commission of the European Communities for the "Code of Practice and Management Guidelines for Trusted Third Party Services"*, Version 1.0, 1993.

– SAA MP75-1996, *Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia.*

– STEINER *et al.:* Kerberos: an authentication service for open network systems in the proceeding winter, *USENIX Conference,* pp. 191-202, 1988.

BADAN STANDARDISASI NASIONAL - BSN
Gedung Manggala Wanabakti Blok IV Lt. 3-4
Jl. Jend. Gatot Subroto, Senayan Jakarta 10270
Telp: 021- 574 7043; Faks: 021- 5747045; e-mail : bsn@bsn.or.id